



Universitat de Lleida

TREBALL FINAL DE GRAU



ESCOLA
POLITÈCNICA SUPERIOR
UNIVERSITAT DE LLEIDA
INSPIRING THE FUTURE

Estudiant: Roger Peralba Pla

Titulació: Grau en Enginyeria Electrònica Industrial i Automàtica

Títol de Treball Final de Grau: Enregistrament i monitoratge remot de dades de sensors utilitzant comunicació sense fils i de llarga distància LoRaWAN al grup bonÀrea.

Director/a: Marcel Tresanchez Ribes

Presentació

Mes: Març

Any: 2021

ÍNDEX

1.	INTRODUCCIÓ.....	8
1.1.	MOTIVACIÓ	8
1.2.	CAS D'APLICACIÓ.....	9
1.3.	OBJECTIUS	11
1.4.	METODOLOGIA.....	12
2.	DISPOSITIUS.....	14
3.	TECNOLOGIES NECESSÀRIES.....	15
3.1.	LORA I LORAWAN	15
3.1.1.	QUÈ SÓN?	15
3.1.2.	COM CONNECTAR-SE A LoRaWAN	16
3.1.2.1.	OTAA i ABP	16
3.1.3.	ARQUITECTURA DE LA XARXA	17
3.1.3.1.	CLASSES LoRaWAN	18
3.1.3.2.	ELEMENTS DE LA XARXA.....	19
3.1.3.2.1.	NODES FINALS	19
3.1.3.2.2.	GATEWAY	20
3.1.3.2.3.	SERVIDOR DE XARXA	20
3.1.3.2.4.	SERVIDOR D'APLICACIONS	20
3.1.4.	SEGURETAT a LoRaWAN.....	20
3.1.5.	APLICACIONS de LoRaWAN	21
3.1.6.	FACTORS A TENIR EN COMPTE EN LA XARXA:.....	21
3.2.	TTN	22
3.3.	Node-RED	24
3.4.	InfluxDB i Grafana.	26
4.	SUPERVISORY CONTROL AND DATA ACQUISITION	28
4.1.	SCADA.....	28
4.2.	ADOPCIÓ D'UN SISTEMA SCADA	31
4.3.	WinCC OA	31
4.3.1.	ARQUITECTURA	32
4.3.2.	ELEMENTS.....	34
5.	ELECCIÓ DE DISPOSITIUS FÍSICS NECESSÀRIS.....	39
5.1.	MULTITECH CONDUIT	39

5.1.1.	IP 67 Base Station	39
5.1.1.1.	Elements del dispositiu	41
5.1.2.	MPower edge intelligence.....	42
5.1.3.	MDot & XDot	42
5.1.4.	DeviceHQ.....	43
5.2.	DRAGINO LHT65	43
5.2.1.	Especificacions dels sensors	43
5.2.2.	Activació i funcions del sensor	44
5.2.3.	Missatge uplink	45
5.2.4.	Connexió a LoRaWAN.....	45
5.2.5.	Programació mitjançant comandes AT	46
5.2.6.	Especificacions del dispositiu	46
6.	PROTOCOLS DE COMUNICACIÓ	47
6.1.	TCP/IP	48
6.2.	UDP.....	50
6.3.	MODBUS.....	50
6.4.	MQTT.....	51
6.5.	OPC UA	52
7.	DISSENY DE LA SOLUCIÓ.....	54
7.1.	Diagrama de la instal·lació	54
7.2.	Gateway	54
7.2.1.	Configuració	54
7.2.2.	Node-RED en Multitech Conduit.....	57
7.2.2.1.	Explicació general.....	57
7.2.2.2.	Nodes configurats i programats	57
7.3.	WinCC OA	61
7.3.1.	Node-RED	61
7.3.2.	InfluxDB	64
7.4.	Grafana.....	68
7.4.1.	Configuració	68
7.4.2.	Eina alertes	73
7.4.3.	Resultat final.....	74

7.5.	Nodes finals: Dragino LHT65	75
8.	CONCLUSIONS	77
9.	TREBALLS FUTURS	79
10.	BIBLIOGRAFÍA	80
11.	ANNEX	83

ÍNDEX D'IL·LUSTRACIONS

Figura 1: Primera opció d'instal·lació del gateway. [1]	10
Figura 2: Segona i final opció d'instal·lació de la gateway. [1]	10
Figura 3: Estructura d'una xarxa LoRaWAN. [2]	17
Figura 4: Canals de comunicació. [3]	19
Figura 5: Interfície visual. [4]	25
Figura 6: Nodes instal·lats per defecte a la gateway Multitech Conduit IP67.	25
Figura 7: Possibles aplicacions d'execució de Node-RED. [4]	26
Figura 8: Esquema general de la arquitectura d'un sistema SCADA. [5]	29
Figura 9: Arquitectura de WinCC OA. [6]	33
Figura 10: Visió general del GEDI. [6]	34
Figura 11: Detalls del GEDI. [6]	35
Figura 12: Editor de Scripts. [6]	35
Figura 13: Modul PARA per a la gestió dels datapoint. [6]	36
Figura 14: Tipus de datapoint. [6]	37
Figura 15: Exemple de drivers utilitzats en un programa de prova. [6]	37
Figura 16: Element per a la configuració d'una alarma dins un datapoint element. [6]	38
Figura 17: Esquema global de la xarxa amb la gateway com a element central. [7]	39
Figura 18: Interior de la gateway.	40
Figura 19: Exterior de la gateway i definicions. [8]	41
Figura 20: : Leds i significat. [8]	41
Figura 21: Dispositiu Dragino LHT65. [9]	43
Figura 22: Cable de programació del sensor. [10]	46
Figura 23: Convertidor USB a TTL CH340G.	46
Figura 24: Protocols de comunicació disponibles a la gateway.	47
Figura 25: Diferència entre UDP i TCP. [11]	50
Figura 26: Arquitectura del protocol MQTT. [12]	52
Figura 27: Diagrama de la instal·lació.	54
Figura 28: Seccions de configuració Multitech Conduit IP67.	55
Figura 29: Node-RED del servidor en la gateway.	57
Figura 30: Objecte del missatge rebut.	57
Figura 31: Payload rebut.	58
Figura 32: Format del missatge.	59
Figura 33: Vista del Change Node.	60
Figura 34: Configuració del node MQTT.	60
Figura 35: Node-RED en la aplicació de WinCC OA.	61
Figura 36: Configuració del node Aedes MQTT broker.	62
Figura 37: Node MQTT in.	62
Figura 38: Node Influxdb out.	63
Figura 39: Missatge d'avís a Telegram.	64
Figura 40: Node Telegram sender.	64

Figura 41: Arquitectura de NextGen Archive. [6].....	65
Figura 42: Vista de la base de dades.	65
Figura 43: Creació del Backend.	66
Figura 44: Nom del Backend.	66
Figura 45: Configuració General del Backend.	67
Figura 46: Configuració de la base de dades al Backend.	67
Figura 47: Creació del grup i política de retenció.	68
Figura 48: Creació del Data Source i importació de la base de dades.	69
Figura 49: Dashboard del projecte.....	69
Figura 50: Creació d'una panell o gràfic.	70
Figura 51: Panell de configuració de dades.....	70
Figura 52: Eina GROUP BY.	71
Figura 53: Desplegable per a la selecció del rang de temps de mostra.	71
Figura 54: Configuracions visuals.	72
Figura 55: Indicador d'estat de bateria.....	73
Figura 56: Indicador de falla en recepció de dades.....	73
Figura 57: Creació d'un canal de notifikacions.....	73
Figura 58: Configuració de la alerta.	74
Figura 59: Monitorització de les dades.	74

ÍNDIX DE TAULES

Taula 1: Arquitectura LoRa i LoRaWAN	18
Taula 2: Especificacions generals de Multitech Conduit IP67 Base Station.	40
Taula 3: Elements adquirits.	42
Taula 4: Especificacions del sensor de temperatura intern.	44
Taula 5: Especificacions del sensor d'humitat intern.	44
Taula 6: Especificacions del sensor de temperatura extern.	44
Taula 7: Estructura del missatge.	45
Taula 8: Especificacions Dragino LHT65.	46
Taula 9: Equivalència entre les capes TCP i OSI.	49
Taula 10: Funció implementada per a la descodificació del missatge.	59
Taula 11: Funció d'alarma mitjançant un bot de Telegram.	63
Taula 12: Nivells de bateria acord a la programació en el programa de descodificació del payload.	72
Taula 13: Comandes per a la utilització del futur Alarm Mode.	75
Taula 14: Nivell de senyal RSSI i significat.	76

CONCEPTES CLAU

LoRa i LoRaWAN:

Tecnologia de comunicació de llarga distància, sense fils i basada en la comunicació de dispositius de camp sense necessitat d'alimentació externa.

Node o dispositiu final:

El concepte de node final o dispositiu final s'utilitzarà al llarg del projecte, aquest farà referència al dispositiu de camp o sensor, que serà l'encarregat de captar la informació desitjada.

Dispositiu inicial:

Dispositiu on es realitzarà el monitoratge i representació de les dades corresponents a la infraestructura.

Passarel·la o gateway:

Una passarel·la o porta d'enllaç és un dispositiu de xarxa encarregat d'interconnectar xarxes que utilitzen diferents protocols. En aquest projecte i degut a que utilitzarem un dispositiu amb més funcions que una passarel·la senzilla o econòmica, s'utilitzarà el concepte de gateway, provinent de l'anglès i utilitzat comunament per al tipus de dispositiu que s'utilitzarà.

Internet of Things:

Per referir-se a la Internet de les coses s'utilitzarà la seva abreviació IoT. Tal com el seu nom indica IoT es refereix a la interconnexió d'objectes que ens envolten en una mateixa xarxa per tal d'automatitzar-ne el seu funcionament.

Payload:

En aquest projecte realitzarem la transmissió de paquets d'informació mitjançant cadenes de caràcters, aquestes cadenes disposaran de capçaleres d'identificació entre altres. Quan ens referim a payload parlarem únicament de la càrrega útil d'aquestes cadenes, que serà el missatge realment previst com podrà ser la temperatura.

Núvol o Cloud:

Sistema d'emmagatzematge de dades a través de servidors localitzats a Internet, a diferència del tradicional emmagatzematge al propi disc dur de la computadora.

1. INTRODUCCIÓ

1.1. MOTIVACIÓ

El projecte que es desenvoluparà en el present document sorgeix de la incorporació de l'autor al món laboral, concretament a l'empresa bonÀrea agrupa la qual els seus inicis daten de 1959 amb les arrels al sector agroalimentari, però que ha anat evolucionant a mesura que ho ha anat fent el món introduint-se en noves necessitats com l'enginyeria, energia i les comunicacions. Entre aquestes necessitats ha estat molt important el desenvolupament d'una enginyeria de qualitat, capaç d'assolir els reptes i necessitats d'una fàbrica amb més de 5.000 treballadors i amb un gran nombre d'instal·lacions de control i processos en constant expansió.

És en aquesta empresa on degut al seu mètode de treball seccionat per departaments he pogut observar el gran nombre de necessitats, millores i aplicacions on és necessària la implicació d'un enginyer. Cal tenir en compte que bonÀrea treballa amb la filosofia de desenvolupar per ella pròpia les seves instal·lacions utilitzant les tecnologies disponibles més adients, això implica controlar des de tot tipus de processos de fabricació a instal·lacions com benzineres o depuradores entre moltes altres. Alhora, quan parlem de tecnologia és important ser conscients de la evolució d'aquesta al llarg dels anys i de la importància d'estar sempre actualitzat i en constant evolució, unes característiques que seran motiu d'aquest projecte.

Així doncs, ja en el món laboral és interessant veure com aplicar els coneixements teòrics que durant quatre anys un ha adquirit, paral·lelament és igual d'important la voluntat d'aprendre nous conceptes i tecnologies que també formen part de l'entorn d'un enginyer per tal de conèixer bé la tecnologia que ens envolta i poder evolucionar juntament amb ella. El projecte que es desenvoluparà en aquest document destaca precisament en aquest últim fet, ja que es pretén donar solució a la necessitat de l'empresa en el monitoratge de dades aplicant una tecnologia nova tant per a l'estudiant com per a l'empresa, la qual caldrà entendre i desenvolupar per tal de realitzar un sistema de control i monitoratge de dades provinents de sensors de forma remota, un projecte que pretén ser complet i ambiciós per a un estudiant i que pot ser una bona aportació per a l'empresa en el control de múltiples processos i situacions.

Des d'un primer moment resulta una gran oportunitat com a estudiant per ser plenament participant del desenvolupament des de zero d'un nou projecte en una empresa, fet que suposa un repte i una oportunitat d'adquirir nous coneixements aprofitant una estructura industrial on altres enginyers podran aportar la seva visió o recomanacions en situacions específiques que ho requereixin. A més a més, el fet de dur a terme un projecte força relacionat amb la telecomunicació i conceptes informàtics no és més que una motivació per encarar un nou repte amb la finalitat d'aplicar i expandir coneixements estudiats durant el grau, però també de relacionar-los i ampliar-los en nous camps relacionats amb l'enginyeria i l'electrònica, comprovant que tots i cadascun d'ells en moltes ocasions estan o poden ser relacionats.

Finalment, un fet tant o més important que l'anterior és que demostrar la viabilitat i utilitat de la proposta d'aquest projecte pot esdevenir en un futur en una gran aportació per a centenars d'aplicacions a l'empresa referents al control de dades de processos varis, les quals dotaran a aquesta d'una millor eficiència en situacions varies, especialment en situacions que puguin ser crítiques i necessitin requisits específics.

1.2. CAS D'APLICACIÓ

La quarta revolució industrial o indústria 4.0 en la qual ens trobem immersos té com a element clau l'automatització dels processos industrials per tal d'obtenir empreses més intel·ligents, les quals puguin gestionar els seus recursos d'una forma més eficient. En aquest projecte s'incidirà en aquesta automatització en el control de dades, un element comú en totes les empreses. Indiferentment del tipus d'empresa que tractem aquesta necessitarà controlar i gestionar certes dades, ja siguin en termes de seguretat, per al control de processos o per estar al corrent de les quotes del mercat on opera. Per tant, un dels elements que formen part d'aquesta revolució industrial és la importància del tractament de les dades, cada vegada més nombroses, amb l'objectiu d'aconseguir una millor gestió i control dels molts elements a tenir en compte en una empresa i el seu entorn. En aquest projecte de prova pilot per a la implantació d'una xarxa LoRaWAN al complex industrial es treballarà únicament en dades referents a estats, concretament en el desenvolupament d'un sistema de monitoratge i control de temperatures per a un sistema d'avís d'incendi en els quadres elèctrics que es troben en l'empresa.

La infraestructura per al control i monitoratge de temperatures en cas d'incendi que es durà a terme en aquest projecte aplicarà un dels conceptes clau en l'anteriorment esmentada indústria 4.0, com és la utilització de la IoT. Aquesta infraestructura té com a finalitat la intercomunicació de dades entre un dispositiu inicial de representació gràfica i un dispositiu final de captació de dades, fent ús del concepte IoT que s'aplicarà mitjançant les tecnologies LoRa i LoRaWAN amb l'ajuda d'una gateway.

Els dispositius que formaran part d'aquesta infraestructura es detallaran en apartats següents, aquests seran un conjunt de sensors com a dispositius finals, una gateway per a la recepció i tractament de dades i software per a l'emmagatzematge i representació d'aquestes. Aquests quatre elements tenen com a finalitat dotar de control l'àrea que ocupa tot un complex industrial de més de 220.000 m², i tot i que en el cas que ens ocupa es treballarà amb temperatures, qualsevol tipus de dada que pugui ser captada per un dispositiu podrà ser monitoritzada amb aquest sistema, com per exemple la humitat o la llum solar incident.

L'element principal a tenir en compte d'aquesta infraestructura serà la gateway, encarregada de rebre les dades de cadascun dels nodes finals i fer-ne la gestió i tractament cap a un dispositiu inicial, fent la funció de passarel·la i alhora de servidor. Per tant, serà de vital importància la correcta configuració i control d'aquest dispositiu.

La instal·lació de la gateway es realitzarà a l'edifici més alt del complex industrial (Fig. 1), el qual alhora és un dels més centrals d'aquest i on el radi de la zona a controlar variarà entre 200 i 400 metres segons la direcció, de forma que atenent-nos les característiques de la tecnologia LoRaWAN no hi ha d'haver inconvenients en la comunicació de dades en termes de distància. Si que serà necessari estudiar la comunicació en termes d'infraestructures entre la gateway i dispositiu final, ja que en llocs limítrofs del complex o subterranis caldrà sobrepassar una gran quantitat d'elements. Per altra banda, l'empresa disposa d'un segon edifici (Fig. 2) amb una altura considerable per instal·lar-hi una gateway d'aquest tipus. Tot i que la proposta inicial era d'instal·lar-ho en aquest, finalment es va prendre la decisió del canvi, ja que el primer cas plantejat es trobava en un dels extrems del complex industrial i podia resultar molt menys eficient. Cal remarcar, però, que serà un punt a tenir en compte en cas d'ampliació de la xarxa.

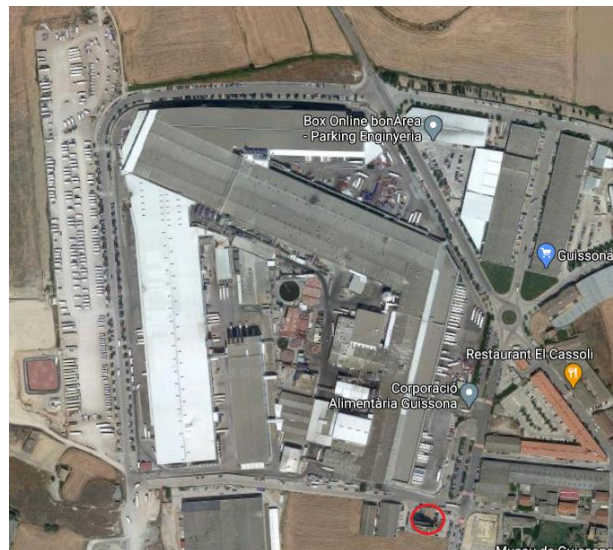


Figura 1: Primera opció d'instal·lació del gateway. [1]

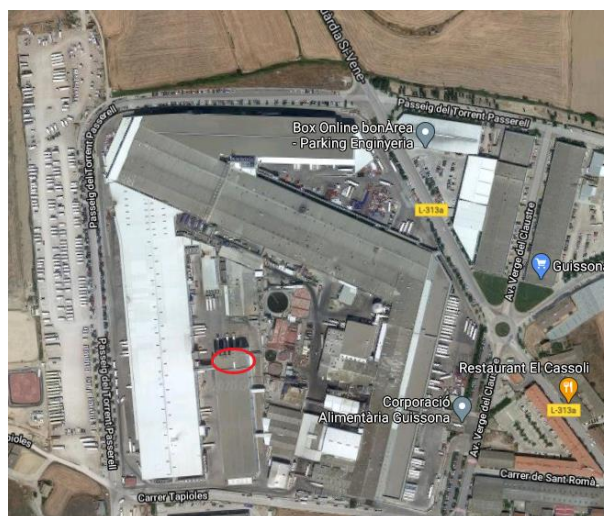


Figura 2: Segona i final opció d'instal·lació de la gateway. [1]

Pel que fa a dispositius finals es disposarà d'un conjunt de sensors de temperatura que utilitzin tecnologia LoRa amb la finalitat d'instal·lar-los en els quadres elèctrics corresponents de la fàbrica, instal·lacions de les quals es vol realitzar el control de temperatura.

Finalment, el dispositiu inicial serà l'encarregat de mostrar les dades monitorades, existeixen diferents opcions segons la necessitat i en el cas d'aquest projecte es preveu aprofitar una estructura SCADA, concretament la de WinCC OA pertanyent a la empresa Siemens i que és el software utilitzat actualment a bonÀrea per als diferents projectes que requereixen monitoratges de processos i interacció HMI (*Human-Machine Interface*). En aquesta estructura SCADA és on es pretén representar i monitorar les temperatures per tal d'obtenir un sistema visual per al monitoratge de temperatures i avisos en cas d'incendi. D'aquesta forma quan en una nau de la fàbrica es detecti alguna temperatura superior a un rang establert l'operari podrà rebre un avís mitjançant SMS, Mail o altre que es definirà durant el transcurs del projecte.

Tot i que cada espai de la empresa bonÀrea agrupa disposa del seu sistema d'alarmes en ple funcionament i complint estrictament la llei i normes de seguretat, és important tenir en compte l'evolució tecnològica. Per aquest motiu resulta interessant evolucionar també tecnològicament com a empresa i actualitzar-se per tal d'aprofitar les noves i més avantatjoses tecnologies, assolint així un nivell de treball cada vegada més eficient en termes de costos, infraestructures i responsabilitat amb el medi ambient. La implantació d'aquesta tecnologia cobra sentit en aquest projecte quan pensem en la velocitat de detecció d'un incendi i l'augment de la seguretat en aquest sistema en un complex de les dimensions de bonÀrea, motiu pel qual s'ha decidit fer aquesta implantació en els quadres elèctrics, elements on degut a la seva infraestructura podrien ser en cas d'incendi l'origen principal del focus, d'aquesta forma s'actuarià d'una forma molt més ràpida en l'extinció del foc. Alhora mitjançant aquesta infraestructura s'aconsegueix un sistema de control de dades que pretén estalviar grans quantitats de material per al cas que ens ocupa i en futures aplicacions, aconseguint així una gran infraestructura de control sense la necessitat de costoses i complexes instal·lacions, sobretot de cablejat. A més a més la tecnologia que es tracta en aquest projecte resulta aplicable en molts àmbits, però cobra especial sentit en casos com el que es pretén tractar, on una superfície de més de 220.000m² podrà ser controlada remotament des de qualsevol dispositiu que pugui admetre la representació o rebuda de dades.

1.3. OBJECTIUS

L'objectiu principal del present projecte és la realització d'una prova pilot de la instal·lació i funcionament d'una xarxa privada LoRaWAN situada al complex industrial La Closa pertanyent al grup empresarial bonÀrea Agrupa, la finalitat d'aquesta instal·lació és permetre realitzar la transmissió i monitoratge de dades entre un dispositiu inicial i un final amb l'ajuda d'una gateway que realitzi el filtratge i enllaç de dades entre nodes. Per assolir-ne la realització es defineixen els següents objectius:

- Realitzar una xarxa privada LoRaWAN amb el mínim d'elements necessaris i la menor complexitat per facilitar tasques d'escalabilitat i manteniment.
- Crear un sistema d'avís d'incendi en cas que es detecti una temperatura fora d'un rang establert.
- Estudiar el monitoratge de temperatures en quadres elèctrics.

Per realitzar aquest procés, però, cal endinsar-se en un conjunt de coneixements força amplis i que són conseqüència d'objectius i passos de caràcter inferior que duren a la consecució d'aquest objectiu final. Per tant, serà de vital importància gestionar bé aquests objectius per tal de definir d'una forma clara i precisa els procediments que caldrà dur a terme a l'hora d'avançar en els passos cap a la consecució de l'objectiu final. Aquests són els següents:

- Realitzar un estudi de mercat i de la tecnologia que pretén ser aplicada per tal d'adquirir els dispositius adients.
- Ser conscients de les necessitats individuals i de funcionament de cadascun dels tres dispositius que formaran el projecte.
- Escollir una correcta comunicació entre els dispositius que pertanyin a la xarxa.
- Realitzar una correcta configuració dels dispositius per assolir-ne el resultat desitjat.
- Aprofitar l'estructura del sistema SCADA de l'empresa, on s'allotja el servidor de producció.
- Evitar la utilització del Cloud o altres plataformes en xarxa.

1.4. METODOLOGIA

La metodologia que es pretén seguir està marcada pels objectius descrits en l'apartat anterior, desenvolupar el projecte en petits objectius facilitarà seguir un mètode de treball adequat i eficient, fent que no es realitzi un pas prèviament a la consecució de l'anterior i evitant així pèrdues d'informació i passos mal realitzats.

Inicialment caldrà fer una recerca exhaustiva d'informació i de mercat de la tecnologia i dispositius que es pretenen utilitzar i les necessitats d'aquesta. Així doncs en primer, lloc serà necessari cercar i disposar d'un sensor de temperatura adient per a l'aplicació que es vol dur a terme, aquest procés no ha de comportar inconvenients, ja que tot i que aquests han d'estar adaptats a una tecnologia molt concreta, aquesta ja està desenvolupada i disposa de varietat de dispositius com han de ser els sensors de temperatura que s'adaptin a aquesta tecnologia. Per tant aquest aspecte del projecte es basarà en cercar informació i contrastar-la correctament per tal d'aconseguir una bona elecció en el dispositiu, degut a que el cas d'aplicació és en una empresa i serà important també establir una relació qualitat-quantitat-preu amb el proveïdor d'aquests, una forma d'optimitzar recursos interessant d'aplicar en casos com el que tractem.

Una vegada es disposi dels sensors adients, caldrà escollir la gateway correctament. Observant el mercat ens podem adonar que hi ha una gran varietat de marques i models diferents en

estoc, però quan parlem d'un dispositiu amb una tecnologia encara no desenvolupada dins l'empresa i per a un projecte de certa importància cal prestar especial atenció en l'ajuda que et poden subministrar tant la marca com el proveïdor a l'hora de resoldre possibles dubtes i conceptes del dispositiu. Encara que pugui semblar un fet de poca importància ja que en els temps en què ens trobem disposem d'informació quan i on volem, és molt important poder consultar directament a experts en el tema en qüestió, són aquests els que et facilitaran informació de primera mà i evitaran pèrdues de temps innecessàries o excessos d'informació poc detallada que puguin dur a confusions. Tant o més important serà la guia del dispositiu, una guia ben detallada pot ser de gran ajuda tan per al client com per al fabricant, ja que el primer disposa d'un lloc on informar-se i on pot intentar resoldre els dubtes per ell mateix i el fabricant evita una aglomeració de qüestions de nivell bàsic.

En ser una tecnologia a comprendre dins l'empresa la metodologia de treball en aquest es basarà en dedicar tantes hores com siguin necessàries a consultar tota la informació d'aquest dispositiu per a continuació començar a experimentar-hi. A mesura que s'aclareixin els conceptes caldrà ser conscient i aplicar criteris objectius per tal d'iniciar-se en la configuració final del dispositiu, que serà la utilitzada en el projecte. Quan es disposi de la configuració desitjada el pas següent serà assolir la comunicació entre els sensors de temperatura i la gateway, aquest punt es realitzarà inicialment amb un sensor, de tal forma que quan es comprovi el funcionament d'aquest sistema de comunicacions restarà afegir la resta dels nodes amb el mètode utilitzat pel primer, per claus de dispositiu.

Finalment i ja que en el software SCADA no serà necessari estudiar-ne les opcions de mercat, es procedirà a cercar el mètode de comunicació més adient entre la gateway i el software SCADA de Siemens WinCC OA, en aquesta comunicació entre gateway i dispositiu inicial hi haurà força protocols de comunicació, per tant caldrà també dedicar les hores necessàries a estudiar i comprendre tots aquests protocols de comunicació per tal de finalment tenir la capacitat d'escollir el més adequat amb les tecnologies disponibles entre la gateway i WinCC OA.

Paral·lelament a l'elecció del mètode de comunicació caldrà també endinsar-se en la extensa arquitectura de WinCC OA, en aquest punt les hores que si pretén dedicar són les necessàries per tal de poder obtenir una bona comprensió. Tot i que es tracta d'un software nou per a l'usuari aquest s'utilitza en l'empresa i per tant es podrà rebre ajuda de primera mà quan sigui necessari, amb la pretensió de reduir el temps que s'hi dediqui, ja que el procediment per entendre dubtes podrà ser més ràpid que en la gateway i nodes finals, on dependrà de fabricant, distribuïdor i fòrums que es puguin trobar.

Així doncs el projecte es podrà dividir en tres fases principals relacionades en la comprensió i correcta gestió dels tres dispositius que s'utilitzaran, també hi haurà dues fases que no seran menys importants que les anteriors, ja que correspondran als protocols de comunicació entre els dispositius. Serà important durant aquest procés tenir temps "il·limitat" per dedicar-hi, ja que facilitarà una bona comprensió de la informació i assegurarà realitzar passos amb total seguretat.

2. DISPOSITIUS

Tal com s'ha descrit en apartats anteriors els dispositius necessaris per a realitzar la instal·lació seran tres, en aquest apartat es detallaran de forma general aquests amb la finalitat d'introduir-los i mostrar una visió general de la instal·lació prèviament a fer-ne una explicació més detallada.

- Sensor:

Existeixen una gran varietat de sensors de temperatura al mercat, també un bon nombre de sensors que tinguin capacitat per treballar amb tecnologia LoRa. L'escollit en aquest projecte és el Dragino LHT65. L'elecció d'aquest ha estat definida per dos motius principals, en primer lloc la recomanació del proveïdor habitual en relació amb la necessitat del projecte i el cost d'aquests, en segon lloc el fet que Dragino sigui una marca amb renom en aquest tipus de dispositius i tecnologia. Tot i que aquest model no disposa de bateria intercanviable el fet que aquesta disposi d'una elevada vida útil no farà d'aquest fet un inconvenient especialment crític, més tenint en compte que l'empresa està desenvolupant un sensor propi. Per altra banda, un element a favor és que disposa de connector per afegir-hi un sensor extern, aportant més funcions i possibilitats al dispositiu.

- Gateway:

Gràcies a la seva escalabilitat la gateway que s'utilitzarà serà el model Conduit IP67 base station de la marca Multitech. A banda de què aquest utilitza tecnologia LoraWAN la elecció d'aquest és deguda a dos motius principals, en primer lloc el seu potencial a nivell de desenvolupament i la capacitat de realitzar la funció de servidor, ja que a banda de les configuracions pròpies d'una gateway disposa d'un petit sistema operatiu amb possibilitat d'afegir-hi aplicacions, entre elles la instal·lada per defecte Node-RED, que permetrà realitzar una programació del mateix pel que respecta al tractament i comunicació de les dades. Per altra banda el fet de tenir una bona infraestructura darrera a nivell d'ajuda en forma de fòrums i distribuïdors és una bona opció alhora de fer front a problemes o problemàtiques que puguin sorgir en aquest.

- Eina de visualització:

Tot i que WinCC OA ve determinat per part de l'empresa és obvi que en l'elecció d'un programa SCADA aquesta va contemplar diferents opcions al seu moment, i per tant la decisió de treballar amb WinCC OA ve fonamentada per raons que l'afavoreixen. Donant un primer cop d'ull a WinCC OA i comparant amb programes del mateix tipus un pot observar sense problemes com realment aquest està força per davant enfront de la competència a causa de la gran infraestructura que aporta i gran nombre de possibilitats que ofereix per a l'automatització. Això sí, caldrà pagar un preu per a tots aquests avantatges ja que pertany a l'empresa Siemens.

3. TECNOLOGIES NECESSÀRIES

3.1. LORA I LORAWAN

3.1.1. QUÈ SÓN?

Durant el transcurs dels anys el món ha anat evolucionant de la mà de la tecnologia, especialment en les últimes dècades, i entre aquestes evolucions ens trobem amb la IoT coneguda com la Internet de les Coses. Les noves aplicacions d'aquesta tecnologia requereixen solucions tècniques òptimes per a aquesta en els diferents escenaris on es pot implantar, i en moltes ocasions les xarxes de connectivitat 3G o 4G poden arribar a ser excessives tant en l'àmbit de cost com d'infraestructura per a aplicacions que no necessiten processos complexos, com pot ser la captura de dades cada cert temps que es pretén tractar en aquest projecte. En la mateixa situació ens trobem quan necessitem implantar IoT en zones on la connexió a Internet tingui restriccions o cobertura escassa, o inclús si tenim pensat realitzar algun tipus de control en zones sense accés a energia elèctrica. Aquesta problemàtica ha pogut ser resolta amb l'aparició de LoRa i LoRaWAN, que permeten un nou ús en la banda lliure de l'espectre de ràdio per crear-hi connexions sense fil a un cost molt baix comparat amb tecnologies com 4G o Wi-Fi.

LoRa significa Long Range i va ser creada el 2009, és una **tècnica de modulació** passabanda anomenada Chirp Spread Spectrum (CSS) utilitzada en comunicacions militars i espacials a casa del seu baix cost, baix consum i la solidesa enfront de interferències, patentada i propietat del fabricant de chips de ràdio Semtech tot i que actualment està administrada per qui desenvolupa LoRaWAN, LoRa Alliance, una entitat sense ànim de lucre. Aquest tipus de modulació sense fil utilitza un ampli espectre de banda de ràdio ISM sense llicència per sota de 1GHz, que a Europa correspon entorn els 868MHz mentre que a Estats Units és de 915Mhz i a Àsia de 433Mhz, fet que li permet tolerar interferències com són el soroll elèctric o l'efecte doppler. Alhora, degut a que disposa d'un ample de banda baix respecte a altres tecnologies com 3G o 4G que el limita per aplicacions com VoIP o videovigilància, el seu consum d'energia és baix. Per altra banda un element limitador és que a Europa la banda de freqüència de 868MHz té dues limitacions, la primera és la regla de l'1% que indica que no podem transmetre dades més de l'1% del temps, es a dir, si enviar un paquet de dades ocupa 100 mil·lisegons haurem d'esperar 900 mil·lisegons a enviar el següent. La segona és que la potència d'emissió no pot superar els 25mW.

Tot i els seus avantatges i inconvenients aquestes característiques fan que LoRa sigui ideal quan necessitem una xarxa facilitadora de IoT per a sensors de tot tipus que necessitin enviar pocs bits d'informació en intervals de temps a partir de segons i en distàncies de fins a 30 quilòmetres. El baix consum d'energia esmentat juntament amb una configuració adequada en el mètode de comunicació dels nodes té com a conseqüència la possibilitat d'utilitzar sensors alimentats amb bateries de tipus botó en períodes amb un màxim entorn dels 10 anys, tenint en compte que hi haurà altres factors implicats en la seva vida útil com poden ser el temps de repòs del dispositiu, el hardware implicat o la temperatura d'operació.

La tecnologia LoRa està prenent importància en l'àmbit de les comunicacions a través de LoRaWAN, un protocol de xarxa de baix consum i àrea extensa que neix de la necessitat d'aplicar la tecnologia LoRa basada en IoT en espais amb condicions adverses a altres tecnologies, en xarxes privades de sensors o actuadors i en instal·lacions locals que requereixen

poca complexitat, esdevenint un estàndard de control de les comunicacions de dispositius sense fil que utilitzin tecnologia LoRa.

LoRaWAN significa Long Range WAN i és el **protocol de xarxa** bidireccional responsable de l'encaminament entre portes d'enllaç i nodes finals, es troba a la capa d'enllaç al medi i utilitza la tecnologia LoRa per comunicar i administrar dispositius IoT que utilitzin LoRa, composta principalment per la gateway i els nodes. La gateway actua com a receptora i/o emissora d'informació des de o cap als nodes finals i possibilita el tractament d'aquesta informació en els dispositius adients segons la necessitat, mentre que els nodes capten o reben aquesta informació.

Així doncs LoRa és la capa física que habilita la comunicació a llarga distància i LoRaWAN defineix el protocol de xarxa i l'arquitectura del sistema.

3.1.2. COM CONNECTAR-SE A LoRaWAN

Per utilitzar aquesta tecnologia Lora amb la finalitat de comunicar dispositius IoT existeixen dos tipus de xarxes. La primera i escollida en aquest projecte és crear una xarxa privada pròpia, serà necessari desenvolupar-la i configurar-la des de zero amb l'avantatge que l'usuari podrà ajustar i adaptar la xarxa a les seves necessitats i li aportarà una major seguretat respecte a una xarxa pública. La segona opció s'implementa a nivell nacional i a dia d'avui disposa de mancances a Espanya, però es basa en utilitzar un operador de xarxa de forma molt similar a les companyies telefòniques, d'aquesta forma es poden contractar companyies evitant haver de fer el manteniment i desplegament de la xarxa però pagant la subscripció a l'operador. Un exemple d'aquesta última n'és Sigfox.

Per altra banda els dispositius finals que s'hauran d'utilitzar en aquesta xarxa utilitzaran LoRa i hauran de registrar-se i activar-se a la xarxa corresponent que utilitzi aquesta tecnologia mitjançant el mètode OTAA o ABP, els quals es detallaran al següent apartat. El procés de registre es realitza directament a la capa d'accés al medi i no en capes superiors per tal d'augmentar la seguretat mitjançant l'ús dels següents paràmetres propis de cada dispositiu i depenent del mètode implementat:

- DevEUI: Direcció del dispositiu.
- AppEUI: Identificador de la aplicació.
- NwsKsKEY: Clau criptogràfica de sessió.
- AppSKey: Clau criptogràfica de sessió d'aplicació.

3.1.2.1. OTAA i ABP

Existeixen dos procediments per registrar dispositius a una xarxa LoRaWAN, aquests són *Over The Air Activation* (OTAA) i *Activation By Personalization* (ABP), on OTAA és el mètode més segur.

En OTAA el dispositiu final ha de seguir un procediment de connexió configurant de forma manual els paràmetres necessaris per a la connexió, que són DevEUI, AppEUI i AppSKey. El procés d'activació s'inicia per part del dispositiu final, que envia un missatge MAC de petició

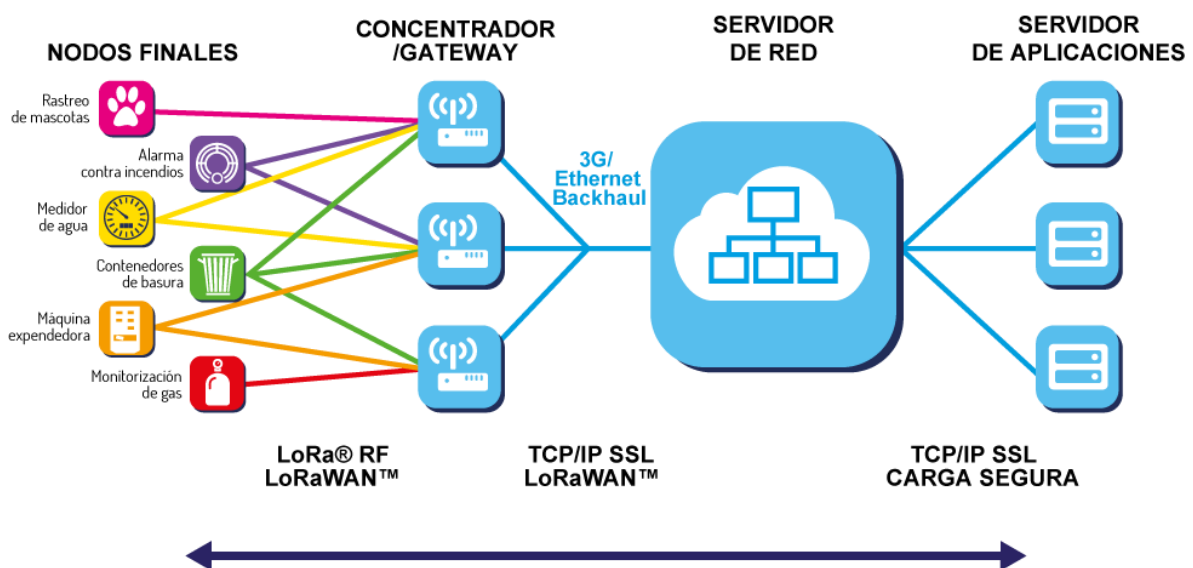
d'unió anomenat *join request* amb el DevEUI i AppEUI i un valor aleatori per evitar filtracions. A continuació el servidor de xarxa respon amb un mateix missatge MAC d'acceptació de la unió si el dispositiu té accés permès a la xarxa, juntament amb unes claus generades que s'emmagatzemen amb la resta al node final, a partir d'aquí el node ja estarà connectat.

En ABP es configuren de forma manual la direcció del dispositiu DevEUI i les dues claus de sessió NwkSKey i AppSKEY, de forma que el dispositiu pot transmetre des del primer moment i serà la gateway qui validarà que les claus corresponguin a la sessió, si no obviarà el missatge. D'aquesta forma s'evita haver de fer un *join request* i rebre una confirmació per part del servidor, un mètode especialment útil en dispositius que puguin estar en moviment o tinguin problemes de recepció.



3.1.3. ARQUITECTURA DE LA XARXA

L'arquitectura d'una xarxa LoRaWAN es compon per tres elements principals que són els nodes finals, la gateway i el servidor de xarxa. Les portes d'enllaç o gateway transmeten els missatges entre dispositius finals i el servidor de xarxa central en una topologia de xarxa anomenada estrella, que indica que els nodes es connecten directament a la gateway, element central. Aquestes portes d'enllaç es connecten al servidor de xarxa a través de protocol IP, mentre que els dispositius finals utilitzen comunicació sense fil LoRa fins a les portes d'enllaç. A més a més aquesta estructura sol estar formada per servidors d'aplicació on es mostren o tracten les dades i on el protocol de comunicació utilitzat varia segons la necessitat de l'aplicació i la varietat de protocols que es disposin, essent alguns exemples el protocol TCP/IP o MQTT entre altres.

A la següent figura (Fig. 3) es mostra aquesta arquitectura típica, caldrà tenir en compte que degut a les característiques de la gateway que s'utilitzarà en aquest projecte ell mateix podrà fer de servidor de xarxa i no serà necessari un servei extra per a realitzar aquesta funció.



Pel que fa a l'estructura de capa de xarxa aquesta és similar al model OSI de xarxes, de forma que LoRaWAN es una capa superior a LoRa i fa la funció de capa d'enllaç, essent LoRa la capa anomenada física (Taula 1). Degut a la tecnologia d'espectre de propagació que s'utilitza, les comunicacions amb diferents velocitats de dades no interfereixen les unes amb les altres, creant així un conjunt de canals virtuals que augmenten la capacitat de les portes d'enllaç, que es distribueixen en diferents canals de freqüència i de velocitat per assolir una bona comunicació entre els dispositius finals i les portes d'enllaç. A més a més per tal de maximitzar la vida de la bateria dels nodes finals i sobretot la capacitat de la xarxa el servidor de xarxa LoRaWAN gestiona la potència d'emissió i la freqüència del canal per a cada dispositiu final de forma individual mitjançant un esquema de velocitat de dades adaptatiu (ADR) en funció de la distància.

	APLICACIÓ			
	LoRaWAN			
	MAC			
	Classe A	Classe B	Classe C	
	LoRa			
	Banda ISM (Industrial – Scientific – Medical)			
	EU 868	EU 433	US 915	AS913

Taula 1: Arquitectura LoRa i LoRaWAN

Aquest tipus de comunicacions de punt final són generalment bidireccionals, això significa que una mateixa gateway pot realitzar funcions tant de receptora com de transmissora d'informació en qualsevol moment, motiu pel qual aquesta tecnologia esdevé útil també per a actuadors a banda de sensors. Una altra característica important d'aquesta xarxa és la difusió selectiva, que permet qualsevol actualització o modificació de software per aire mitjançant l'enviament de paquets d'informació a múltiples destinataris de la xarxa.

Un altre punt a tenir en compte és la transmissió asíncrona d'informació, quan aquesta és transmesa per un node final és rebuda per múltiples portes d'enllaç, que envien aquests paquets de dades a un servidor de xarxa centralitzat que els filtra evitant així duplicar la informació, alhora realitza comprovacions de seguretat i gestiona la xarxa. Finalment aquesta informació podrà ser transmesa als servidors d'aplicació.

3.1.3.1. CLASSES LoRaWAN

Els nodes finals de la xarxa LoRaWAN disposen de tres classes de canals bidireccionals possibles i cadascun d'aquestes s'utilitza per optimitzar la comunicació entre el dispositiu final i la gateway segons el consum energètic i la capacitat de recepció, aquestes classes són la A, B i C (Fig. 4).

Els dispositius configurats en classe A són els més bàsics i tenen capacitat d'enviar dades en intervals de temps o quan ocorre algun esdeveniment, com per exemple que una temperatura sobrepassi el valor límit establert. Aquest tipus d'operació afavoreix que els dispositius que treballen en aquesta classe tinguin un menor consum d'energia però tenen l'inconvenient de necessitar transmetre un enllaç ascendent *uplink* abans de rebre un enllaç descendent

downlink. És a dir, cada vegada que el dispositiu envia un paquet es té l'oportunitat de rebre'n un, d'aquesta forma podem enviar un canvi d'estat a un actuator si ens envia un paquet que mostra un estat incorrecte. Així doncs els dispositius amb aquesta classe seran ideals per a aplicacions que no acostumin a rebre dades, *downlink*, sinó enviar-les, *uplink*.

Els dispositius en classe B tenen la capacitat de rebre dades, *downlink*, sense necessitat de fer una emissió prèvia, *uplink*, d'aquesta forma es poden enviar paquets als dispositius de forma programada. La forma d'aconseguir aquest funcionament és mitjançant "beacon", una tecnologia bluetooth de baixa energia i que no necessita sincronització prèvia, motiu pel qual el consum d'energia d'aquesta classe de dispositius és superior als de classe A.

Els dispositius de classe C permeten la recepció de dades *downlink* contínua des de la gateway, ja que sempre està actiu excepte quan el dispositiu final està transmetent una dada *uplink*. Tot i que aquesta classe proporciona els millors temps de resposta i capacitat de transmissió des del servidor pràcticament en tot moment, degut a la seva operativitat energèticament són els dispositius menys eficients i necessiten fonts d'energia constants per operar.

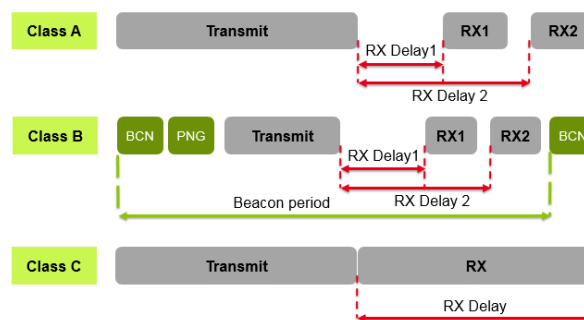


Figura 4: Canals de comunicació. [3]

3.1.3.2. ELEMENTS DE LA XARXA

3.1.3.2.1. NODES FINALS

Els dispositius o nodes finals són sensors o actuadors connectats a la gateway on hi envien la informació que aquests capturen, tota aquesta informació és rebuda a través de la gateway al servidor de xarxa i finalment per mitjà d'una interfície d'aplicacions o API arriba a la aplicació final per a l'usuari. Ja que l'arquitectura del protocol de comunicació té com a característica la bidireccionalitat, en el cas dels actuadors aquest procés es pot realitzar a la inversa fent que aquests puguin rebre comandes d'actuació.

És interessant fer èmfasi en aquests nodes finals ja que són els elements físics que dotaran a les instal·lacions de les finalitats que aquestes necessitin, ja sigui per a control de temperatures, humitats o qualitat de l'aire entre altres aplicacions. Aquests dispositius físics de hardware poden ser de més o menys complexitat en el seu funcionament, però tots necessiten com a element comú un mòdul de ràdio per a la transmissió de dades mitjançant LoRa i de capacitats de detecció de variables que els permetin actuar almenys com a sensors.

3.1.3.2.2. GATEWAY

Com ho són els nodes finals aquest també és un dispositiu físic imprescindible per desenvolupar la xarxa de comunicacions LoRaWAN, aquest és l'encarregat de fer de passarel·la o porta d'enllaç i gestionar simultàniament els canals per on es rep la informació convertida en bits. Per entendre-ho d'una forma més senzilla realitza la funció d'antena per a la recepció i emissió de paquets de dades, amb la tecnologia que comporta tot això. El poder computacional de la gateway és limitat i tota la complexitat i intel·ligència d'aquest procés generalment el trobem al servidor de xarxa.

3.1.3.2.3. SERVIDOR DE XARXA

Tota la informació i paquets de dades tractats per la gateway són rebudes per un servidor de xarxa, on es realitzen els processos de tractament de les dades ja que aquest servidor s'encarrega de:

- Encaminament o reenviament de missatges a l'aplicació adequada.
- Seleccionar la millor porta d'enllaç per al missatge d'enllaç descendent, típicament en funció de la qualitat RSSI que indica la intensitat de la senyal rebuda i la SNR que indica la senyal de soroll dels paquets rebuts anteriorment.
- Eliminació de missatges duplicats si es reben per múltiples portes d'enllaç.
- Desxifrar els missatges enviats des de nodes finals i encriptar els missatges que s'envien als nodes.

En aquest servidor de xarxa hi ha connectades les portes d'enllaç o passarel·les, en aquest cas de la gateway mitjançant el protocol IP (Internet Protocol), en algunes ocasions degut a que la xarxa conté una interfície per a la porta d'enllaç es permet que el proveïdor de la xarxa administri aquestes portes i controli situacions d'error.

3.1.3.2.4. SERVIDOR D'APLICACIONS

En aquests servidors és on finalment s'aplica la IoT, ja que és on es realitzen els processos útils amb les dades recopilades pels dispositius finals. Aquests servidors s'executen de forma pública o privada interactuant amb el servidor de xarxa LoRaWAN i realitzen el processament de l'aplicació. Són varies les aplicacions que es poden dur a terme amb les dades recopilades i serà qüestió de l'usuari depenent de la finalitat de les dades escollir l'aplicació més adient, des de la representació de dades a un programa en una interfície visual fins a missatges o avisos mitjançant SMS o Email entre altres.

3.1.4. SEGURETAT a LoRaWAN

Fins ara s'havia parlat de les característiques d'aquesta xarxa LPWAN que es pretén implementar i els seus grans avantatges, però cal tenir en compte un element molt important quan parlem de xarxes de comunicació, que és la seguretat a l'hora d'operar en aquesta i

evitar així filtracions o pèrdues de dades. Així doncs, mantenir una bona privacitat i control de les dades és element indispensable d'una bona xarxa de comunicacions.

En l'apartat 2.1.2. d'aquest projecte s'ha descrit els dos possibles mètodes per connectar-se a una xarxa LoRaWAN, un més segur que l'altre, i és amb els conceptes introduïts en aquest com podem entendre el sistema de seguretat d'aquesta xarxa que es fonamenta en l'autorització d'autenticació entre equips, d'un node final a la xarxa. Per altra banda la seguretat de les dades transmeses es basa en un esquema de seguretat utilitzat en aquest tipus de xarxes de clau compartida simètric, és a dir, s'utilitza la mateixa clau per xifrar i desxifrar la informació, fet que implica que les dues parts del procés han de ser coneixedores d'aquesta clau confidencial. El mètode utilitzat per xifrar és l'algoritme AES de 128 bits, que en l'actualitat no és vulnerable a atacs per força bruta. Per tal de resoldre futurs problemes de seguretat en la confidencialitat d'aquesta clau, LoRaWAN utilitza altres claus de xifrat derivades de la principal junt a un valor aleatori, fet que impossibilita intrusions a la xarxa.

3.1.5. APLICACIONS de LoRaWAN

Amb tot el descrit anteriorment som coneixedors que estem davant una tecnologia aparentment amb molt potencial i que pretén revolucionar la comunicació de dades especialment en zones on anteriorment a la indústria 4.0 hi havia força dificultat. Per tal de reforçar els conceptes anteriors i mostrar la capacitat real d'aquesta tecnologia a continuació s'anomenen algunes de les aplicacions que es poden dur a terme a banda de la qual es pretén implantar en aquest projecte:

1. Xarxes de sensors varis en ciutats, camps o indústria dedicats a aparcaments, senyalitzacions o il·luminació.
2. Xarxes IoT on no sigui necessari transmetre veu o vídeo, unes transmissions que estan en desenvolupament però a priori no són recomanables.
3. Seguiment de vehicles, animals o persones mitjançant geolocalització.
4. Control de nivells d'humitat i/o temperatura en activitats com l'agricultura o la meteorologia.
5. Control de la pol·lució.
6. Mesures de gas, aigua, electricitat o altres.

3.1.6. FACTORS A TENIR EN COMPTE EN LA XARXA:

A continuació es detallaran els principals factors a tenir en compte en el desenvolupament de la xarxa que es pretén, tot i els avantatges d'aquesta tecnologia caldrà ser conscients també de les seves limitacions per tal de poder crear una instal·lació altament eficient i respectuosa amb la tecnologia que es vol implantar, així doncs caldrà tenir en compte els següents punts:

- Cicle de treball: Caldrà respectar la norma de l'1% i per això es podran adoptar diferents mesures. En primer lloc serà necessari fer una bona gestió del període de transmissió de dades dels dispositius, i a ser possible utilitzar un sistema que prioritzi un enviament de dades instantani quan el sensor detecti un canvi de valor brusc, d'aquesta forma serà possible augmentar el període de transmissió en situació normal. Un altre factor a tenir en compte en relació a aquesta norma serà la mida del missatge, com més gran sigui aquest més temps estarà en transmissió i menys temps d'enviament tindrem per dia. Similar ens passarà amb la distància del node a la gateway, a major distància major temps d'enviament i a l'inrevés.
- Nombre de dispositius: Un altre factor a tenir en compte per al disseny de la xarxa serà la capacitat d'aquesta en el nombre de dispositius, com més dispositius més càrrega i menys rendiment de la xarxa tindrem. Segons les característiques de la xarxa podrem arribar fins a 5.000 dispositius finals si la mida del missatge ronda els 10 bytes.
- Distància a la passarel·la: Tot i que la xarxa LoRaWAN és escalable, a mesura que augmenta el nombre de dispositius allunyats a la passarel·la disminueix l'efectivitat de la xarxa.
- Reconeixement per part de la gateway: Ja que la gateway pot enviar missatges de reconeixement o comprovació d'estat dels dispositius finals, aquest fet pot influir en el nombre d'enviament de dades per part de la gateway per dia.

3.2. TTN

The Things Network coneguda com a TTN es una iniciativa iniciada l'any 2015 a Amsterdam per part de Wienke Giezeman i Johan Stokking, actualment TTN és el principal proveïdor de codi obert de servidors de xarxa de LoRaWAN, un servei global de dades de la IoT de xarxa descentralitzada construïda i administrada pels mateixos usuaris que permet que qualsevol usuari pugui connectar els seus nodes utilitzant gateway que formin part de la xarxa o afegint-los en aquesta.

Per accedir a aquest servei s'utilitza la seva pàgina web <https://www.thethingsnetwork.org/> on l'usuari necessitarà registrar-se de forma similar a la resta de pàgines web amb un compte d'usuari, una vegada s'accedeixi a la consola principal aquesta estarà dividida en dues parts principals, aplicacions i gateways, que podran ser configurades en els seus apartats corresponents sempre que disposem i hi connectem un o ambdós dispositius.

Aplicacions serveix per integrar aplicacions com Node-RED a TTN amb la finalitat d'utilitzar les dades rebudes dels nostres sensors, una forma molt efectiva per poder organitzar diferents projectes d'una forma clara i configurar aquests independentment segons la necessitat. Dins de cada aplicació cal haver registrat cada node mitjançant l'apartat *register device*, una

vegada amb el node registrat podrem accedir a *manage devices* per tal de veure o modificar les dades dels nodes registrats. Per altra banda a l'apartat gateway podrem afegir el nostre dispositiu que farà de passarel·la entre els nodes finals i The Things Network i fer-ne un petit control d'informació com l'estat, localització o els missatges enviats o rebuts.

Com s'ha esmentat en apartats anteriors, un servei de xarxa sense seguretat no tindria cap mena de sentit, per tant The Things Network té en compte diversos factors que tot i ser una xarxa pública la fan altament segura. En primer lloc utilitza un servei similar a VPN, on cada usuari pot accedir només a les seves dades i escollir si és necessari amb qui compartir-les, per altra banda cada node i cada aplicació disposen dels seus propis identificadors i claus que actuen sobre el procés de comunicació des del node final fins al servidor aconseguint un xifrat d'extrem a extrem, finalment i per tal de millorar encara més la seguretat TTN no emmagatzema cap tipus de dades rebudes, en cas que necessitem guardar aquestes serà necessari un altre servei dedicat explícitament a aquest emmagatzematge com pot ser Microsoft Azure.

Així doncs TTN aporta diversos avantatges com són:

- Utilitzar LoRa en una localització on ja hi ha una gateway connectada a TTN, només necessitaràs els mòduls per afegir a aquesta xarxa.
- Capacitat d'accedir a les dades des de qualsevol indret amb connexió a Internet i a temps real.
- Capacitat de compartir les teves dades o unir-se a xarxes existents d'una forma molt senzilla.
- Facilitat d'afegir nodes al sistema.

Ara que es coneix TTN ens podem preguntar la necessitat d'utilitzar aquesta plataforma en aquest projecte en lloc d'una xarxa privada on comuniquem els nostres nodes directament mitjançant connexió punt a punt. Doncs bé, en el desenvolupament d'aquest projecte va ser un recurs inicial per tal de realitzar les primeres proves de connexions, però a mesura que es va anar adquirint coneixement en els conceptes i dispositius utilitzats es va arribar a la conclusió que TTN no tenia viabilitat en aquest. En primer lloc la voluntat de crear una xarxa privada pròpia de l'empresa el menys exposada possible a interferències o manipulacions feia de TTN una opció poc viable, per altra banda i degut a que aquest no té capacitat per a emmagatzemar dades la necessitat d'un servei extra per realitzar aquest procés augmentava la infraestructura de la instal·lació, no respectant un dels eixos principals d'aquest projecte com és realitzar la instal·lació amb el mínim d'elements possibles per tal de minimitzar al màxim la complexitat de la xarxa.

3.3. Node-RED

Node-RED és un entorn de programació visual Open Source, dissenyat per enginyers de IBM amb la finalitat de solucionar la complexitat a l'hora d'integrar el hardware amb altres serveis, consolidat en la gestió i transformació de dades a temps real en entorns basats en la indústria 4.0 com ho és la IoT degut a la senzillesa tant en el seu aprenentatge i ús com la seva robustesa i necessitat de pocs recursos de còmput, donant possibilitat a utilitzar tecnologies complexes sense la necessitat de profunditzar-hi personalitzant només la capa inicial.

Node-RED opera localment al navegador mitjançant el port 1880 en una interfície visual de programació, que a diferència de la majoria d'entorns de programació aquesta està basada en fluxos utilitzant la programació mitjançant nodes, una forma molt intuïtiva de realitzar programacions complexes per comunicar hardware i serveis i que simplifica en gran mesura la programació respecte a la que coneixem com a tradicional. En aquest cas, els nodes difereixen del concepte de nodes finals esmentats en apartats anteriors i són etiquetes que realitzen cadascuna d'elles funcions específiques que tenen definides, per tant l'usuari només haurà de precisar algunes variables o realitzar algunes adaptacions al node corresponent. Per exemple, si volem enviar dades a una adreça de correu electrònic, caldrà un node que rebí o creí aquestes dades i l'ajuntarem amb el node destinat a correu electrònic, configurat ja per a aquesta funció i on només li haurem de definir principalment l'adreça de correu electrònic de destí. Així doncs, obtindrem una programació relacionant dos nodes amb finalitats concretes que mitjançant el mètode de programació tradicional requeriria una bona depuració i constaria de diverses línies de codi, implicant molt més temps de desenvolupament i un augment de recursos de computació. Per altra banda i per satisfer necessitats no cobertes, Node-Red disposa de la creació de nodes altament personalitzables o destinats a la programació de funcions pròpies de l'usuari, sempre dissenyats amb llenguatge JavaScript.

A banda dels nodes instal·lats per defecte a l'aplicació Node-RED, on cadascun d'aquests forma part d'alguna de les llibreries disponibles, Node-RED consta d'un conjunt de llibreries disponibles per instal·lar, per tant si es necessita algun node extra o per alguna funció més específica com podrien ser bases de dades o protocols de xarxa, aquests es poden instal·lar sempre que hi hagi disponible la llibreria corresponent ja que al ser un projecte Open Source és la mateixa comunitat la que desenvoluparà nous codis font. Així doncs, també existeix la possibilitat que l'usuari creí els seus propis nodes. Tot i que aquest cas no serà objecte d'estudi en aquest projecte i està detallat en diferents guies, la forma principal per a la creació d'un node és mitjançant un fitxer HTML i un JavaScript amb la configuració i la lògica del node que es vulgui dissenyar.

Pel que fa a la seva interfície visual (Fig. 5) a l'esquerra de la pantalla podem trobar tots els nodes que hi ha per defecte i les llibreries instal·lades posteriorment, aquests nodes estan separats segons la seva categoria (Fig. 6) i poden diferir en instal·lacions de Node-RED segons el dispositiu i la seva finalitat. A la part central trobem la interfície per crear el nostre flux de codi, de forma que s'executarà mitjançant els esdeveniments de cada node en el sentit que aquests estiguin programats. Finalment, a la part dreta trobarem diferents zones que mostraran informació sobre cada node o la consola de *debug*, on es mostren els missatges que arriben al node *debug* corresponent, útil per comprovar el correcte funcionament del programa a l'hora de transmetre i tractar les dades. També a la part dreta trobarem un polsador que indica *Deploy*, aquest serveix per guardar els canvis realitzats al codi i

desplegar l'aplicació al servidor de forma que aquesta quedarà activada fins que l'usuari la pari o vulgui modificar.

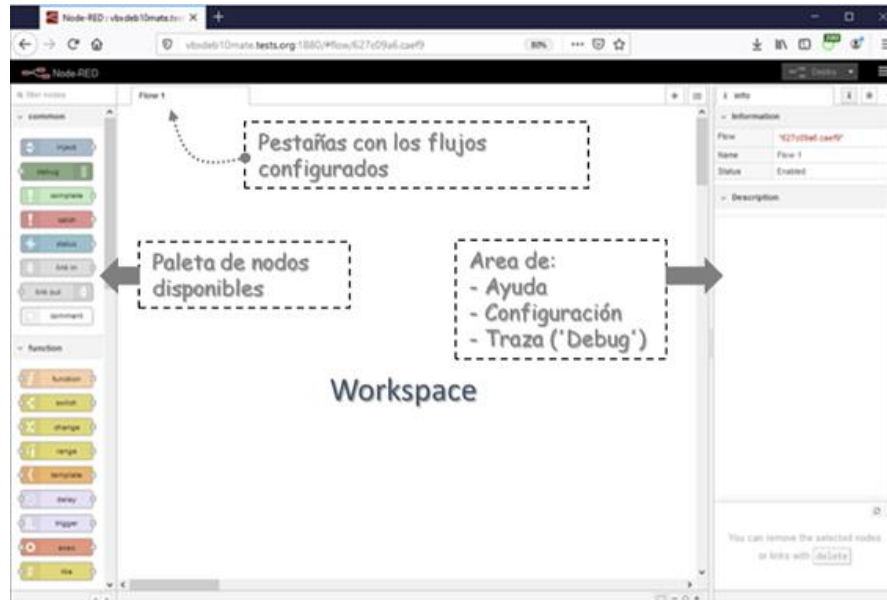


Figura 5: Interfície visual. [4]

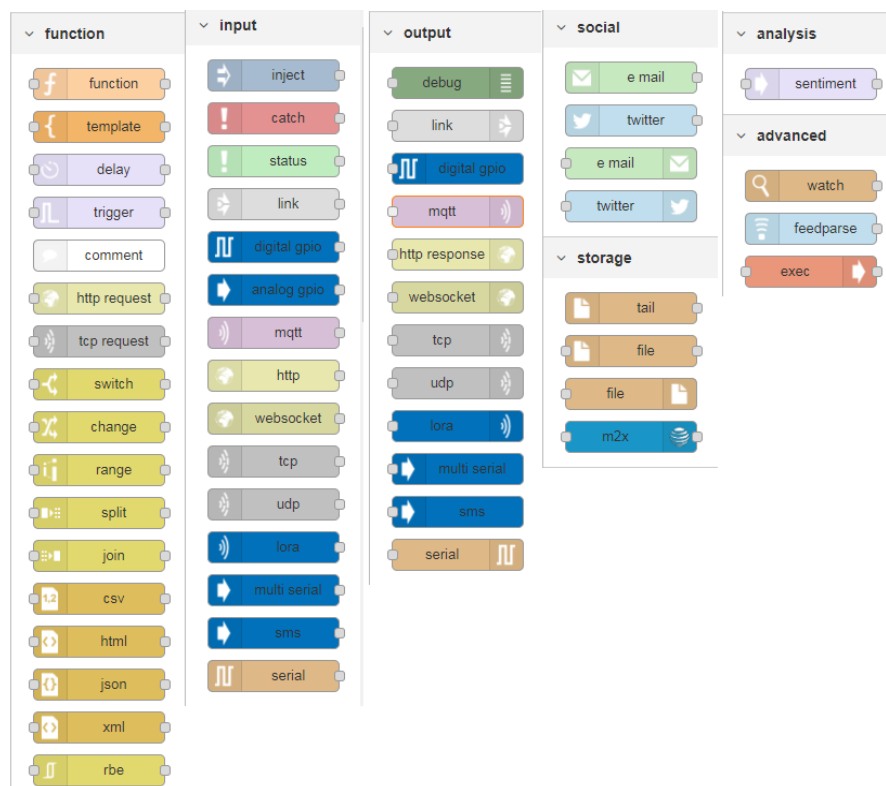


Figura 6: Nodes instal·lats per defecte a la gateway Multitech Conduit IP67.

El seu model basat en entorn de programació Node.js, un motor d'execució asíncron de JavaScript per a servidors el fa ideal per executar-se en maquinari de baix cost connectat a la xarxa en dispositius com Raspberry Pi, Arduino o Android i al cloud com per exemple Microsoft Azure, Amazon Web Services o IBM Cloud. A més a més el seu emmagatzematge mitjançant arxius JSON facilita la seva importació o exportació a l'hora de compartir els fluxos en equips de treball o altres.



Figura 7: Possibles aplicacions d'execució de Node-RED. [4]

3.4. InfluxDB i Grafana.

InfluxDB pertany a Influx Data i és un sistema per a la creació i gestió de bases de dades, és un software de codi obert gratuït tot i disposar de versió de pagament. Es tracta d'un software concebut per a bases de dades temporals (TSDB o Time Series Data Base) que, com el seu nom indica, emmagatzema grans quantitats de sèries de dades ordenades en el temps. A diferència de les bases de dades relacionals les TSDB aporten una major velocitat en l'emmagatzematge i processament de dades juntament amb les corresponents marques temporals, un fet que ha pres importància amb la popularització de la IoT i Big Data. Per altra banda InfluxDB sobrepassa els esquemes SQL i NoSQL ja que aquest permet l'anàlisi de les dades a temps real.

Pel que fa al seu funcionament aquest es basa mitjançant les comandes corresponents a la consola de comandes on s'executi aquesta, tot i que el podem utilitzar amb eines de visualització. Per altra banda en l'àmbit estructural en destaquen els següents punts:

- **Bases de dades:** Contenedor on s'emmagatzemaran les dades amb les sèries temporals associades, també els usuaris i polítiques de retenció entre altres.
- **Política de retenció (RP):** InfluxDB ens permetrà establir la política de retenció de dades, és a dir, escollir quant temps volem que es guardin les nostres dades a la base corresponent.

- Measurements: Estructura on s'emmagatzemen les dades i que identifica la seva finalitat. Per exemple si mesurem temperatures podrem definir els nostres Measurements com a Temperatures.
- Tags: La informació que emmagatzemen els tags correspon als valors indexats dins aquest camp de la base de dades. Per exemple el tag Temperatura_exterior identificarà les temperatures exteriors.
- Field: Mètriques i valors associats a un timestamp de la base de dades.

De la mateixa forma que InfluxDB, Grafana és també un software lliure que permet la representació i visualització de sèries de dades provinents de bases de dades temporals. Així doncs, aquesta eina permet la representació de les dades escollides de la nostra base de dades representant-les segons la nostra necessitat dins un gran ventall d'opcions. Per altra banda possibilita l'ús d'avisos per a valors que sobrepassin un rang establert mitjançant eines com Email, Telegram, SMS o Microsoft Teams.

El seu funcionament és molt senzill, en primer lloc seleccionarem d'on volem obtenir les dades i el nom de la base de dades corresponent, així com la direcció del servidor on aquestes s'emmagatzemin. A continuació l'usuari ja podrà personalitzar la seva eina de visualització en el format desitjat, i haurà d'escollir en cada zona la configuració corresponent d'on vol extreure la informació, quina vol representar i si vol realitzar algun tipus de modificació en alguna dada així com en el format de representació d'aquestes.

4. SUPERVISORY CONTROL AND DATA ACQUISITION

4.1. SCADA

SCADA prové de l'acrònim Supervisory Control and Data Acquisition i tal com el seu nom indica aquest software d'interfície gràfica format per diferents tecnologies o aplicacions s'utilitza per controlar, supervisar i optimitzar processos industrials de forma remota o local mitjançant dispositius instal·lats en planta com poden ser sensors, autòmats PLC o actuadors. A banda de permetre el monitoratge de dades també pot arribar a permetre la interacció amb aquestes entre humà i màquina per tal de realitzar modificacions a l'hora de solucionar problemes o interactuar als processos, aportant un pas més a l'automatització dels processos industrials.

La supervisió és un dels elements principals pel que destaca SCADA respecte a altres tecnologies, supervisar implica realitzar una inspecció superior que orienti o corregeixi les accions que es desenvolupen, veure algun fet amb atenció o sotmetre un esdeveniment a un nou examen per corregir-lo i reparar-lo permetent una acció sobre aquest esdeveniment revisat. Així doncs, a banda del control dels processos aquesta eina de supervisió dotarà de grans avantatges a un procés industrial. Per altra banda l'optimització dels processos es podrà realitzar en diversos sentits, en primer lloc el fet de monitorar un procés i facilitar-ne el control reduirà la necessitat que una persona física comprovi que el procés es desenvolupa correctament. A més a més i amb relació al cas anterior, el fet de disposar de més dades de control i històrics d'aquestes serà molt més fàcil solucionar possibles errors o detectar possibles millores en el sistema.

L'estructura d'aquest sistema es basa en microordinadors com controladors lògics programables PLC, unitats de terminal remotes RTU, controladors d'automatització programables PAC o driver's que es comuniquen amb màquines, dispositius, sensors o similars mitjançant un sistema de supervisió informàtic. Posteriorment aquests microordinadors envien la informació que reben a l'ordinador que disposa del sistema SCADA corresponent. Així doncs, per norma general disposarem del següent hardware i software (Fig. 8):

- Terminal Mestre o sistema de supervisió (MTU): Ordinador principal del sistema que acostuma a ser un PC encarregat de supervisar, recollir i processar les dades per controlar qualsevol error dels servidors, també és l'encarregat d'enviar les instruccions. El sistema SCADA més senzill és el que utilitza un únic ordinador anomenat MTU que supervisa tota la estació.
- Terminals Remots (RTU): Ordinadors industrials de control ubicats a punts estratègics que obtenen informació de les subestacions o accions concretes del procés i l'envien a sistemes de control superiors. És a dir, reben les senyals dels sensors o actuadors de camp i les envien als elements finals de control de l'aplicació SCADA, de forma que estan en un nivell d'automatització inferior a les MTU i a un superior dels sensors o

- similars. Actualment per tal de minimitzar costos s'utilitzen controladors lògics programables gràcies al seu nivell d'integració i major potència de càlcul de la CPU.
- Controlador lògic programable (PLC): Controladors dissenyats per rebre i emetre múltiples senyals tant d'entrada com de sortida per tal d'automatitzar, controlar i captar informació de processos industrials com el control de maquinària i encarregats d'enviar o rebre aquesta informació de/a l'ordinador amb software SCADA. S'utilitzen com a dispositius de camp degut ja que aquests són més econòmics, versàtils i configurables que les RTU.
 - Xarxa de comunicació: Xarxa per on es transmet tota la informació del sistema mitjançant mètodes de comunicació que utilitzen Ethernet, wifi o fibra òptica. El protocol més comú és el TCP/IP, el qual s'explicarà en apartats posteriors.
 - Software: Nucli principal d'un sistema SCADA, sent el programa que processa tota la informació i té la capacitat de convertir-la en interfícies gràfiques i a l'inrevés.
 - HMI: Significa Human-Machine Interface i acostuma a formar part d'un SCADA, és la interfície home-màquina que trobem mitjançant un panell de control on operador i procés estan comunicats interactivament mitjançant la representació de dades del procés a l'humà donant possibilitat a l'operador d'actuar sobre el procés o màquina o visualitzar dades per tal que observi el monitoratge. Cal destacar que hi ha sistemes HMI que per ells sols no esdevenen un SCADA.
 - Sensors i actuadors: Igual que els PLC són instruments de camp, els sensors són dispositius utilitzats com a detectors de magnituds o variables del sistema mentre que els actuadors tenen la capacitat d'actuar sobre un altre dispositiu mecànicament.

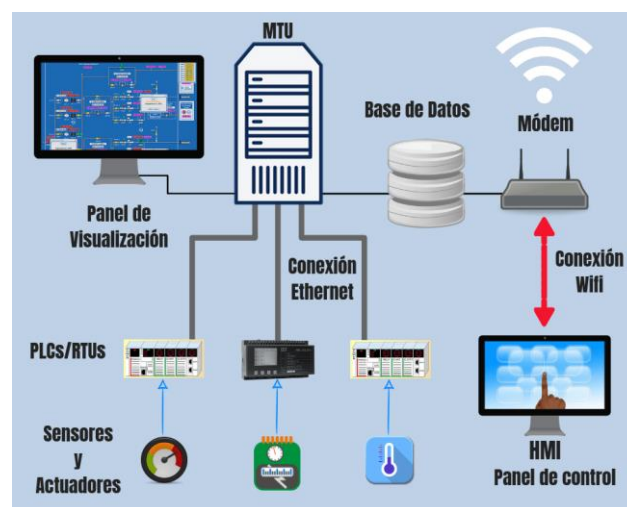


Figura 8: Esquema general de la arquitectura d'un sistema SCADA. [5]

En vista els seus avantatges i estructura robusta aquest sistema s'ha instaurat a la indústria amb el temps per tal de controlar els processos productius d'una forma molt més ràpida, concreta i directa, ja que amb aquest es poden controlar dades i estats de tot tipus d'instal·lacions a temps real i en un mateix dispositiu. Per aquest motiu especialment en la indústria 4.0 SCADA desenvolupa un paper fonamental per esdevenir indústries més productives degut a la major eficiència i un millor control dels equips, allargant en moltes ocasions la vida útil d'aquests amb l'ajuda de l'anàlisi permanent de dades que permet prevenir i anticipar errors.

Finalment i per tal de deixar detallats els enormes beneficis d'aquest sistema, es descriuen a continuació:

- Supervisar remotament o localment instal·lacions i equips.
- Retroalimentació en temps real mitjançant la lectura del que passa als processos i sistemes amb opció de mostrar-ne els comportaments a través d'imatges dinàmiques.
- Generació d'històrics de dades i emmagatzematge de registres de dades (*big data*) per al processament, generació d'informes o representació gràfica i la presa de decisions comparant amb dades anteriors.
- Augment de la productivitat degut a la capacitat de realitzar un control centralitzat.
- Augment de la qualitat i eficiència ja que es poden diagnosticar estats de màquines i processos a temps real.
- Augment de la seguretat ja que el sistema permet crear i administrar alarmes i registres d'incidències quan es duu a terme alguna acció, amb el corresponent augment en la seguretat dels treballadors de planta.
- Solució de problemes a distància.
- Escalable i flexible degut a la capacitat de modificar-se per afegir-hi recursos o integracions de dispositius.
- Programació d'esdeveniments i accions automàtiques. Per exemple si una temperatura sobrepasa un límit establert podem programar un avís SMS.
- Augment de la productivitat.
- Assignar permisos d'accés per controlar l'accés de diferents usuaris.

4.2. ADOPCIÓ D'UN SISTEMA SCADA

El grup empresarial bonÀrea disposa d'una àmplia trajectòria industrial la qual ha anat desenvolupant tecnològicament adoptant diverses solucions, una d'aquestes és els sistemes SCADA per a l'esquematzació i monitoratge de les numèriques instal·lacions industrials que trobem a l'empresa, facilitant així multitud de processos que es duen a terme i millorant l'efectivitat d'aquests, repercutint directament en el benestar dels treballadors, especialment els de manteniment i reparacions, que van observar en primera persona el canvi d'haver de desplaçar-se contínuament a les instal·lacions per conèixer el seu estat a poder conèixer l'estat d'aquestes des d'un monitor.

EL desenvolupament d'aquesta tecnologia ha resultat indispensable per a l'evolució de l'empresa, però com tota tecnologia aquesta evoluciona, per aquest motiu ha resultat necessari adaptar-se i seguir aquesta evolució per tal de repercutir en la millora de l'empresa. Inicialment s'utilitzava software de tipus IDE (Entorn Integrat de Desenvolupament), un entorn de programació sense llicència comercial i del qual es va intentar realitzar una programació partint des de zero per desenvolupar un software que desenvolupés funcions SCADA, un resultat final que no va assolir les expectatives desitjades per a la implantació en unes instal·lacions cada vegada més complexes i nombroses. Paral·lelament, es van utilitzar altres sistemes basats en software comercial com WinCC de Siemens amb uns resultats força positius tot i algunes limitacions.

Ambdós sistemes van quedar obsolets i van arribar als seus màxims en termes d'escalabilitat, és per aquest motiu que l'any 2018 es planteja l'adopció d'una nova tecnologia que s'adapti a la infraestructura que pretén adoptar l'empresa, de tal forma que els nous projectes ja es desenvolupessin en aquesta i els anteriors es poguessin anar substituint. Per dur a terme aquest procés es va contactar amb el principal fabricant de PLC utilitzats a l'empresa, de tal forma que la integració entre tecnologies resultés el més eficient possible. Finalment doncs, la solució escollida va ser WinCC Open Architecture de Siemens, un programa que pretenia i pretén aportar un gran salt qualitatiu als diferents àmbits respectius de l'empresa, com l'automatització i control, el manteniment i l'eficiència.

4.3. WinCC OA

Prèviament al desenvolupament d'aquest punt cal fer constar que WinCC OA és una eina amb gran potencial per a la indústria i que a conseqüència el seu domini total requereix multitud de coneixements que cal desenvolupar a mesura que s'hi treballa, inclús amb l'ajuda de formacions pròpies de Siemens. És per aquest motiu que en aquest apartat no es detallarà el global de les funcions específiques de les que disposa aquest sistema, que en són un gran nombre, i es descriurà amb el màxim detall possible una idea general que s'ha adquirit tenint en compte que l'usuari l'utilitzarà per primera vegada i per a una funció molt específica, com és la recepció de dades per part d'una gateway.

SIMATIC WinCC Open Architecture abreviat com a WinCC OA forma part de la família SIMATIC HMI de Siemens, dirigida a aplicacions amb alts requeriments de personalització per part de l'usuari en el control i supervisió d'instal·lacions industrials. Aquest paquet de software està dissenyat per a l'automatització en l'àrea d'operació i control de plantes mitjançant estacions de treball amb capacitats gràfiques. Permet també la representació dels estats momentanis d'un procés i la possibilitat de transferir-hi condicions i comandes mitjançant el

teclat, ratolí o altres dispositius d'entrada interactiva amb resposta immediata a la pantalla. Una altra de les funcions principals d'aquest paquet és el seu sistema d'alarmes en cas de condicions crítiques establertes, juntament amb l'accés a l'històric de dades.

Els aspectes més destacats d'aquest software són:

- Elevat rendiment en sistemes de control redundants i de xarxa, garantint una comunicació constant entre camp i estació de control.
- Orientació a objectes que permet elevada flexibilitat i escalabilitat al sistema aportant una enginyeria eficient.
- Capacitat de fins a 2040 servidors o subsistemes.
- Creació de sistemes d'un sol usuari fins a sistemes distribuïts i redundants.
- Independent de la plataforma i amb disponibilitat per a Windows, Linux, iOS i Android.
- Sistema de recuperació.
- Amplia gamma de controladors i opcions de connexió com són Ethernet/IP, DNP3, IEC 61850/61400, IEC 60870-5-101/104, Modbus, TCP/IP, OPC UA, OPC, XML, S7-1500, S7-1200 o Simatic S7.

Tot i la complexitat de WinCC OA una vegada implementat correctament es simplifica enormement la gestió industrial agrupant en una sola pantalla una vista unificada de processos industrials juntament amb alarmes o alertes de possibles incidències en aquests processos. A més a més aquest fet sol comportar un estalvi econòmic important a les empreses.

4.3.1. ARQUITECTURA

En les tecnologies de l'automatització la disponibilitat i la fiabilitat adquireixen cada vegada més importància, ja que una petita avaria pot esdevenir en elevats costos i riscos en la seguretat d'una instal·lació. La redundància és un dels elements clau que s'utilitza per garantir la gestió de plantes sense efectes adversos, evitant entre altres la pèrdua de dades i/o problemes associats. La configuració exacta del sistema redundat depèn de requisits segons el cas, tot i que el més comú és la duplicació de software mitjançant l'anomenat hot-standby, on s'utilitza dos servidors connectats entre si, ambdós funcionant permanentment, un sempre actiu i l'altre sincronitzant les dades amb la unitat principal, de forma que si el servidor principal o actiu falla el sistema canvia automàticament al servidor passiu o redundant, que agafa el control i esdevé servidor actiu. El resultat d'aquest sistema és que l'accés sempre està garantit.

Una altra opció també utilitzada en sistemes complexos és la modularitat, es basa en utilitzar una xarxa de servidors per a diferents instal·lacions gestionada per un servidor central, de forma que el client té la possibilitat d'accedir a l'estat de les seves instal·lacions des del servidor corresponent o el central. WinCC OA permet disposar d'un sistema de fins a 2048

subsistemes, de forma que cadascun pot aportar funcions addicionals al sistema central o duplicar-les per raons de seguretat, com en el cas anterior.

L'estructura de WinCC OA consisteix en managers (Fig. 9), programes autònoms comunicats entre ells a través de TCP/IP que s'encarreguen d'executar cadascun d'ells una funció específica. Els managers principals són:

- **Event Manager (EV):** El cervell de WinCC OA, s'encarrega d'organitzar les tasques del sistema.
- **Data Base Manager (DB):** Gestiona la base de dades i la introducció de nova informació.
- **Driver Manager (D):** Encarregat de vincular processos i controladors.
- **Control Manager (CTRL):** Processa els programes escrits en CTRL, llenguatge de programació dels scripts de WinCC OA.
- **User Interface Manager (UI):** Interfície on l'usuari observarà gràficament l'estat de tots els processos.

Amb els managers podem diferenciar entre client i servidor, els clients seran managers destinats a processar informació per a la visualització i els servidors seran els encarregats de processar informació i esdeveniments.

Finalment, un altre element a destacar és l'orientació a esdeveniments, de forma que generalment el sistema només processa dades quan es produeix algun canvi en aquest fent ús del Event Manager. Aquesta característica ajuda a reduir el consum de recursos del sistema.

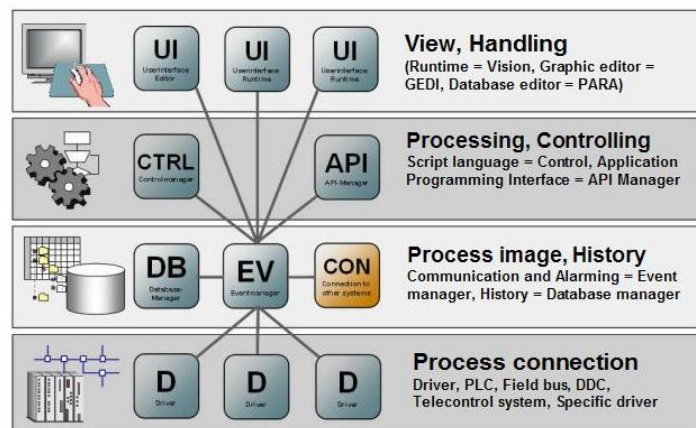


Figura 9: Arquitectura de WinCC OA. [6]

4.3.2. ELEMENTS

GEDI:

Gedi és l'editor on es troben totes les eines per crear, configurar i editar objectes gràfics que poden representar sistemes simples o complexos mitjançant conjunts d'objectes. Els objectes creats en aquest editor s'hauran d'enllaçar posteriorment als anomenats datapoint creats al mòdul PARA, que s'explicarà a continuació. Aquest editor està format per les següents zones (Figs. 10 i 11):

- Project view: Hi podem observar els panells, scripts, llibreries i imatges del nostre projecte.
- Panel Window: És l'àrea de treball on es dibuixen i editen els objectes gràfics.
- The property sheet: Mostra les propietats dels panells, objectes gràfics i referències en un espai per editar i configurar de forma més directa les propietats d'aquests.
- Catalog window/Toolbar: Mostra tota classe d'objectes i referències que serveixen de model o objecte, de forma que es poden arrossegar directament a l'editor.
- Script Editor: Eina per crear i editar els scripts i llibreries, amb llenguatge CTRL (Fig. 12).

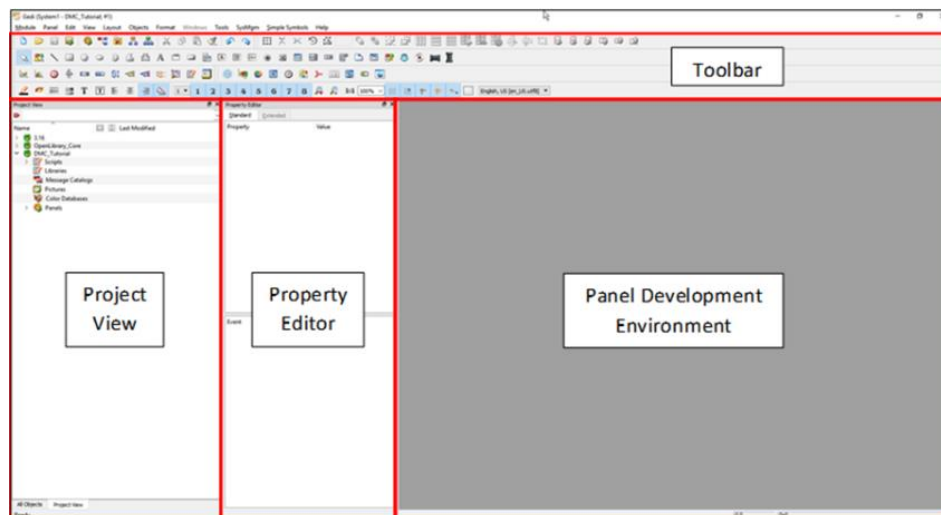


Figura 10: Visió general del GEDI. [6]

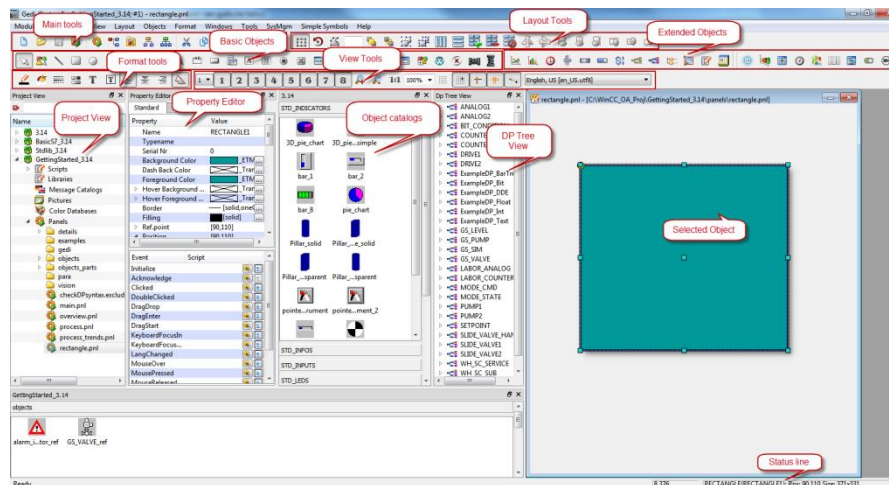


Figura 11: Detalls del GEDI. [6]

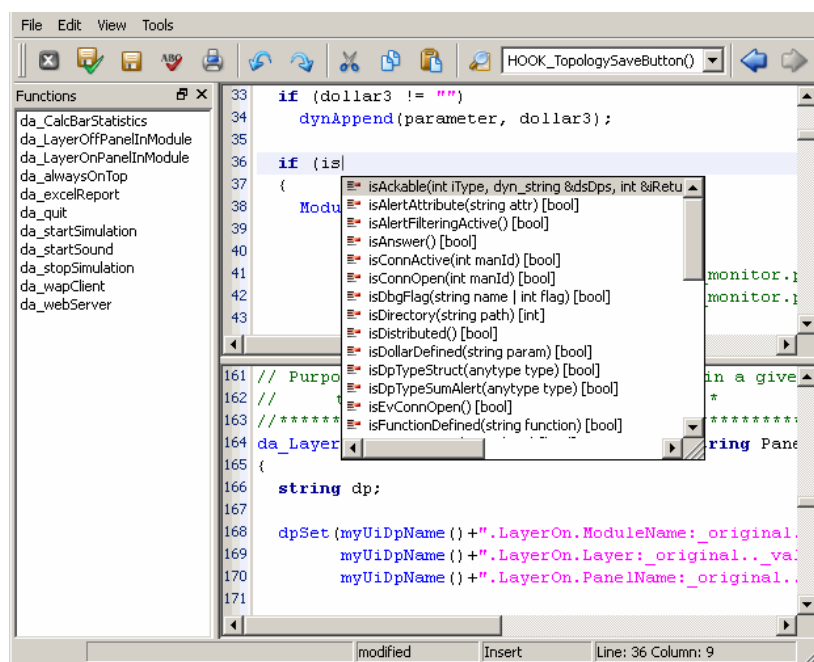


Figura 12: Editor de Scripts. [6]

PARA:

Para (Fig. 13) pertany al manager *User Interface* i es troba dins el Gedi, és una eina utilitzada per crear i editar els anomenats *Datapoint*, guardats en la capeta db (database), on hi ha la base de dades i s'hi poden realitzar canvis simultàniament. Existeixen diferents estructures de datapoints (Fig. 14) que serveixen cadascuna per funcions concretes, aquestes són les següents:

- **Datapoint type (DPT):** Un datapoint type és l'estructura formada per varis elements i que servirà de base per a derivats d'aquesta. Entre dos tipus de vàlvules o de petits motors ens podem trobar que només canviïn certes parts o elements, així doncs el datapoint type representarà l'estructura d'aquests elements que només s'hauran d'adaptar amb petits canvis en algun dels seus elements.

- Master Datapoint (MP): A diferència del datapoint type que especifica l'estructura, el Master Datapoint especifica la configuració d'aquestes estructures generals, aquesta configuració es anomenada PowerConfig i representa combinacions de configuracions més específiques.
- Datapoint element (DPE): Les estructures més senzilles les quals acostumen a ser objectes únics, cada DPE correspon a un valor o estat.
- Datapoint (DP): Derivats dels datapoint types aquests pertanyen a parts concretes del sistema format pel Datapoint Type, representant parts reals dins un sistema de control. Un datapoint conté un o més elements d'un datapoint element.
- Data point attribute (DPA): A més a més del valor representat en temps real aquest conté altres atributs com l'estat, l'origen o el temps.

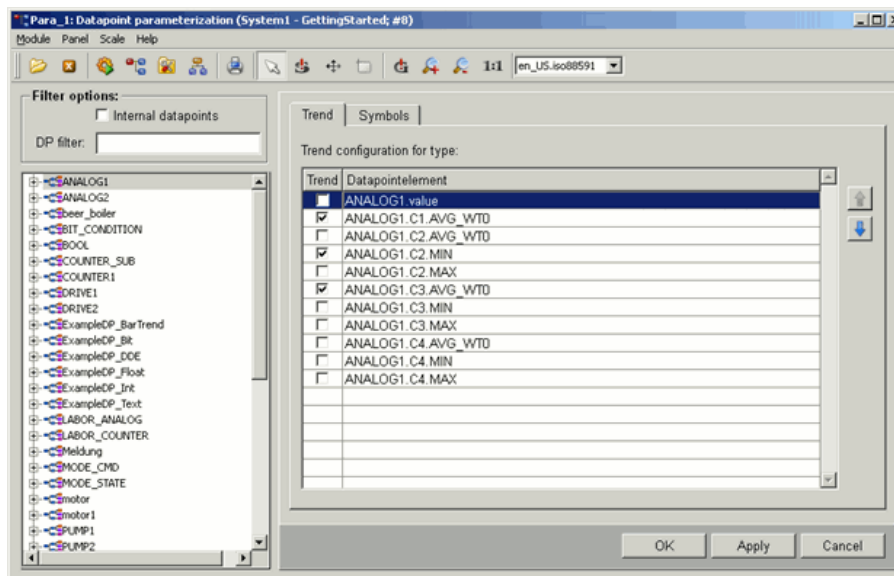


Figura 13: Modul PARA per a la gestió dels datapoint. [6]

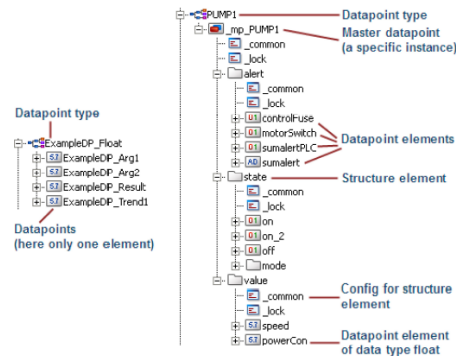


Figura 14: Tipus de datapoint. [6]

DRIVERS:

Els divers o controladors (Fig. 15) són mòduls encarregats de convertir determinats protocols al mètode intern de comunicació de WinCC OA, establint la comunicació entre el control de l'estació i l'automatització. Aquests llegeixen els estats actuals, valors mesurats o comptadors de camp i passen les comandes i/o valors als controladors subordinats. Existeixen diversos tipus de drivers depenent del protocol utilitzat, alguns exemples d'aquests són:

- Ethernet: Modbus TCP, Industrial Ethernet (S7), Ethernet IP (AB).
- Field bus: Profibus.
- Telecontrol system: SSI (Ethernet), IEC 60870-5-101, IEC 60870-5-104...Entre altres.
- Multivendor interfaces: OPC DataAccess, OPC Alarms&Events.

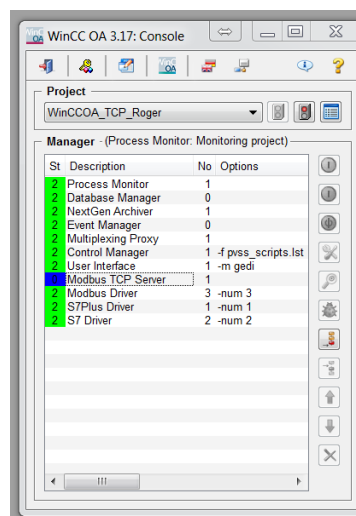


Figura 15: Exemple de drivers utilitzats en un programa de prova. [6]

ALARMES (alertClass):

Una altra de les característiques fonamentals de WinCC OA és el seu sistema d'esdeveniments o alarmes el qual es pot activar als datapoint element sempre que aquests emmagatzemin l'últim valor rebut i que actua mitjançant el manager Event Manager, motor principal del sistema i que realitza un processament de dades quan hi ha un canvi no esperat al sistema. Un avantatge d'aquest sistema és que en algunes programacions SCADA es pot evitar el processament de dades continu i activar aquest quan es detecti un comportament fora d'un rang de valors o esdeveniments establert.

Aquestes senyals d'alerta poden ser contínues o discretes, és a dir que mentre els elements binaris disposaran de dos estats els elements analògics tindran un rang que caldrà especificar. Per tal de configurar-les és necessari accedir a l'editor de bases de dades PARA i afegir la configuració corresponent al sistema d'alertes entre els cinc tipus de classes que existeixen epr defecte, que són Advanced alarm, alert, danger, disturbance, information i warning.

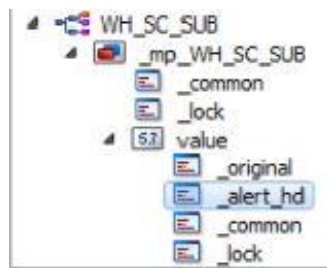


Figura 16: Element per a la configuració d'una alarma dins un datapoint element. [6]

5. ELECCIÓ DE DISPOSITIUS FÍSICS NECESSÀRIS

5.1. MULTITECH CONDUIT

Per tal de realitzar el procés de comunicació entre els nodes finals i el node inicial mitjançant LoRaWAN resulta necessària la utilització d'una gateway amb aquesta tecnologia. En aquest projecte s'utilitzarà la gateway Multitech Conduit IP67 Base Station, aquesta és el model amb més prestacions i més escalable amb tecnologia LoRaWAN per a un ús industrial de la marca Multitech, referent mundial i que permet la gestió dels dispositius LoRa i el tractament de les dades directament a la pròpia gateway ja que pot realitzar la funció de servidor, a diferència d'altres que simplement reenvien les dades a un servidor LoRaWAN extern amb el desenvolupament i cost que això pot comportar. A més a més una qüestió de gran importància en projectes d'aquestes característiques és el suport tècnic que l'usuari final pugui rebre per part de la companyia per tal de solucionar problemàtiques o problemes de desenvolupament, i en aquest cas Multitech disposa d'una bona infraestructura.

5.1.1. IP 67 Base Station

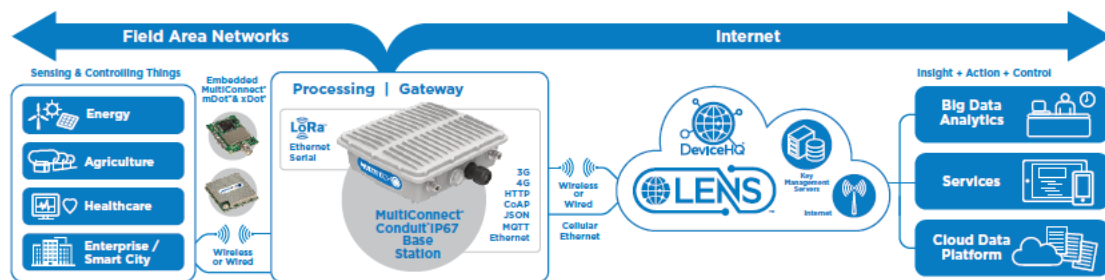


Figura 17: Esquema global de la xarxa amb la gateway com a element central. [7]

Multitech Conduit IP67 és una gateway compatible amb LoRaWAN dissenyada específicament per treballar en exteriors en xarxes LoRaWAN tant públiques com privades i amb una capacitat per a connectar-hi aproximadament fins a 5.000 nodes finals LoRaWAN (Fig. 17). Aquesta doncs és una útil solució per connectivitats LoRa on controlar àrees extenses amb un baix consum en aplicacions IoT

La darrera paraula en la seva nomenclatura, IP67, fa referència a la norma que segueix aquest model Conduit per ser apte en exteriors, així doncs seguint la norma IP el número 6 ens indica una protecció total enfront la pols i el número 7 la capacitat de submergir-se fins a 1m i durant 30 minuts en aigua. A més a més, segons el fabricant aquest resisteix calors extremes, forts vents, neu i humitat.

Conduit disposa de connectivitat 4G-LTE, 3G, 2G i Ethernet per a la seva plataforma d'administració. També disposa de Wi-Fi, Bluetooth i ranures per afegir-hi targetes pròpies de Multitech anomenades mCard per afegir noves funcionalitats la gateway. En la següent taula (Taula 2) es detallen les seves característiques principals.

PARÀMETRES	
Alimentació	PoE 37-57 Volts DC
Rang de temperatura d'operació	-40° C a +70° C
Rang de d'humitat d'operació	20%-90% RH
Banda ISM	868 MHz a Europa
Bandes de freqüència	Ethernet, 4G, 3G, 2G
Velocitat de transmissió de dades	Downlink: 150 Mbps Uplink: 50Mbps
Antenes	LoRa, GNSS, mòbil
Funcions TCP/IP	FTP, SMTP, SSL, TCP, UDP
Emmagatzematge	Micro SD
Connectors	Ethernet, USB, Micro SIM

Taula 2: Especificacions generals de Multitech Conduit IP67 Base Station.

Pel que fa a l'estructura del dispositiu (Fig. 18) internament disposa de la placa base i tots els elements que formen el dispositiu, pel que fa a l'exterior (Fig. 19) observem els diferents connectors per a les antenes al voltant de l'estructura i en el punt central inferior els connectors USB i Ethernet juntament amb els leds (Fig. 20) que ens indicaran l'estat de la gateway.



Figura 18: Interior de la gateway.

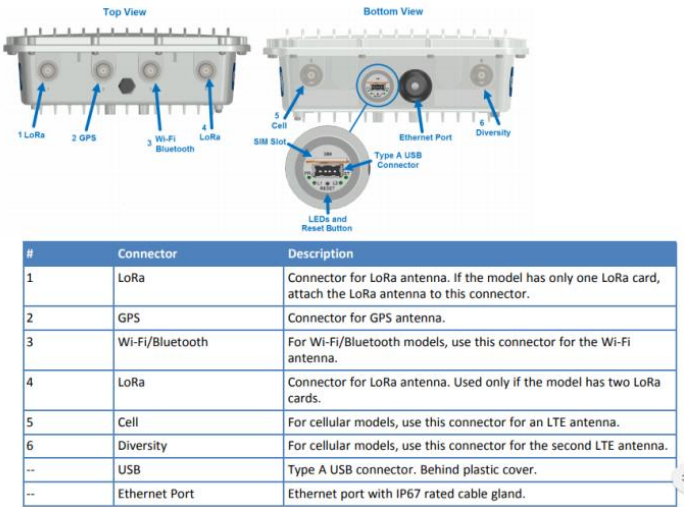
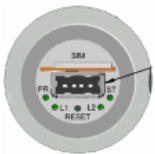


Figura 19: Exterior de la gateway i definicions. [8]

LEDs



Label	LED	Description
PR	Power	Green when powered up.
ST	Status	Red with blinking green. User programmable.
L1	LoRa 1	User-defined. Can be red or green.
L2	LoRa 2	

mPower LED Notes






For mPower models

- The default state of the L1 and L2 LEDs depends on the cellular connection (connected/disconnected) and signal strength.
- To change the LED behavior modify the script /sbin/led_cd_ss.

Figura 20: : Leds i significat. [8]

5.1.1.1. Elements del dispositiu:

En l’adquisició d’una gateway Multitech Conduit el comprador té la possibilitat d’elegir entre alguns components segons la finalitat que aquest li vulgui donar al dispositiu, en la taula següent (Taula 3) es detallen els components del model adquirit que pertanyen al kit anomenat accessory kit.

Element	Imatge
MTCDTIP Base Station	
Antena LoRa externa Omnidireccional	
Antenes LTE i Wi-Fi	
Antena GPS/GLONASS	
PoE	

Taula 3: Elements adquirits.

5.1.2. MPower edge intelligence

Per tal de ser una gateway escalable en solucions IoT i aportar un alt nivell d'administració per part de l'usuari mitjançant múltiples opcions de configuracions, programacions i seguretat entre altres, aquest disposa d'un software integrat anomenat mPower Edge Intelligence, i és a partir del qual en aquest projecte es realitzarà la configuració desitjada per al nostre sistema de monitoratge, una configuració que serà detallada en apartats següents.

5.1.3. MDot & XDot

Aquests mòduls de radiofreqüència aporten connectivitat de llarg abast i transport de dades de pocs bits per a sensors i actuadors basats en IoT seguint la comunicació LoRaWAN, proporcionant una comunicació bidireccional capaç d'assolir distàncies de fins a 15 quilòmetres en camp obert i línia recta i entre 3 i 5 quilòmetres entre edificis.

Alhora mDot té la capacitat de controlar aplicacions escrites i compilades en línia reduint la necessitat d'utilitzar radiofreqüència i/o software extra al sistema, suportant un gran nombre d'interfícies.

5.1.4. DeviceHQ

DeviceHQ és la primera plataforma IoT de la indústria pròpia de Multitech i basada en el núvol per a la interacció M2M entre aplicacions i els dispositius d'última generació de Multitech i el monitoreig remot en per exemple actualitzacions o modificacions de dispositius. Disposa d'una bona quantitat d'eines com la localització, resum configuracions realitzades i l'actual amb els arxius respectius i tractament d'aplicacions que no seran objecte d'estudi en aquest projecte.

5.2. DRAGINO LHT65

El model LHT65 de Dragino és un sensor de temperatura i humitat dissenyat per treballar amb la tecnologia LoRaWAN. Un factor important esmentat en els apartats LoRa i LoRaWAN és la capacitat en aquesta tecnologia d'utilitzar sensors sense fil degut al seu poc consum i la llarga duració de la bateria, un punt que s'ha tingut en compte en l'elecció d'aquest sensor, que disposa d'una bateria de 2400mAh no recarregable però amb una vida útil estimada d'uns 10 anys. Un altre punt a favor d'aquest sensor és que disposa de 3200 registres de data i hora, que poden ser recuperats per al seu anàlisi.

Internament està format per un sensor de temperatura i humitat SHT20 però a més a més externament disposa d'un connector per afegir sensors externs varis com de temperatura, humitat del sòl o inclinació entre altres. En el cas del nostre projecte utilitzarem aquest connector extern per a un sensor de temperatura amb la finalitat de millorar la precisió en la lectura dels valors, així doncs disposarem de la temperatura del sensor intern del dispositiu i la temperatura del sensor extern, que serà lleugerament més precís que el sensor intern. La temperatura interna s'utilitzarà per comprovar que ambdós llegeixen valors en un rang força similar. Per altra banda disposarem del sensor d'humitat, degut a que aquesta dada no serà objecte d'estudi en aquest projecte, ens serà útil a nivell orientatiu i per disposar d'una informació més completa.



Figura 21: Dispositiu Dragino LHT65. [9]

5.2.1. Especificacions dels sensors

En aquesta secció es resumiran les principals especificacions de cadascun dels tres sensors dels quals disposarà el dispositiu, sense entrar en detall en el disseny d'aquests ja que són dispositius comuns sense tecnologies especials.

SENSOR DE TEMPERATURA INTERN	
Resolució	0.01 °C
Precisió	Typ ± 0.3 °C
Long Term Drift (Derivació a llarg termini)	< 0.02 °C/yr
Rang d'operació	-40°C ~ 125°C

Taula 4: Especificacions del sensor de temperatura intern.

SENSOR D'HUMITAT INTERN	
Resolució	0.04 %RH
Precisió	Typ $\pm 3\%$ PH
Long term drift (Derivació a llarg termini)	< 0.02 °C/yr
Rang d'operació	0 ~ 100 °C

Taula 5: Especificacions del sensor d'humitat intern.

SENSOR DE TEMPERATURA EXTERN	
Resolució	0.0625 °C
Precisió entre -10°C to +85°C	± 0.5 °C
Precisió entre -10°C to +85°C	± 2 °C
Rang d'operació	-55 °C ~ 125 °C

Taula 6: Especificacions del sensor de temperatura extern.

5.2.2. Activació i funcions del sensor

El funcionament del sensor LHT65 és força senzill, quan està activat aquest té dos modes d'operació que són els següents:

- 1) Mode hibernació: Quan el sensor no té activada cap connexió LoRaWAN aquest mode és utilitzat per emmagatzemar dades per tal d'augmentar la vida útil de la bateria.
- 2) Mode treball: Quan el sensor actua com a sensor LoRaWAN per afegir-se a la xarxa i enviar les dades al receptor, entre cada emissió el sensor està en mode "descans" on té un consum igual al del mode hibernació. Aquest mode descans no implica que el sensor no estigui treballant, sinó que està esperant a haver de captar una nova dada.

Per altra banda disposem del polsador ACT en la part inferior del sensor que s'utilitza per a les següents funcions:

- Enviament de lectura instantani: Aquesta funció s'activa quan premem el polsador entre 1 i 3 segons, si el sensor està dins una xarxa LoRaWAN enviarà el paquet de dades amb les lectures del moment en què hem premut. Si tenim un sensor extern connectat s'il·luminarà el led blau, si no tenim cap sensor extern s'il·luminarà el led vermell, ambdós momentàniament segons el cas.
- Activació del dispositiu: Pressionant el polsador més de 3 segons el led verd s'activarà i desactivarà 5 vegades, a partir d'aquest instant el sensor entrarà en mode treball per

connectar-se a la xarxa LoRaWAN i s'activarà el led verd altra vegada durant 5 segons una vegada connectat a la xarxa.

- Desactivar el sensor: Pressionant intermitentment en 5 ocasions el polsador ACT s'encendrà el led vermell durant 5 segons, indicador que el sensor entrarà en mode hibernació.

5.2.3. Missatge uplink

El payload de transmissió de dades cap a la gateway conté un total de 11 bytes on els sis primers tenen valors variables en cada dispositiu, el setè defineix el model de sensor extern si és que aquest està connectat i la resta de bytes el valor del sensor extern (Taula 7).

Size (bytes)	2	2	2	1	4
Valor	Nivell de la bateria: 00(b): Esgotant-se 01(b): Baix 10(b): Correcte 11(b): Excel·lent	Temperatura Interior	Humitat Interior	*Ext #	*Ext value

Taula 7: Estructura del missatge.

*EXT # : Model del sensor extern

*Ext value: Valor del sensor extern, si hi és.

La descodificació del payload en aquest projecte es realitzarà mitjançant l'aplicació Node-RED pròpia de la gateway, on mitjançant un script adaptarem el missatge al format que s'adapti millor en aquest cas.

Per altra banda disposem de la rebuda de missatges al sensor o downlink, en aquest cas el led s'activarà en color lila. Hi ha diferents comandes que realitzen les seves funcions corresponents quan s'envien al sensor, com per exemple la configuració del període de mostreig, neteja de la memòria o ajustar l'hora. Aquestes comandes no s'aplicaran en aquest projecte.

5.2.4. Connexió a LoRaWAN

A l'embalatge del sensor podrem trobar una etiqueta amb les diferents claus del sensor segons s'utilitzi el mètode de connexió OTAA o ABP. Per defecte aquest està configurat amb el mètode desitjat, que és OTAA i per altra banda realitza la comunicació en Classe A.

Una vegada introduïdes les claus al servidor el sensor està llest per connectar-se a la xarxa, sempre que activem aquest, i començar a transmetre dades en un període per defecte de 10 minuts. Tot i ser un fet poc habitual, en cas que sigui el nostre servidor qui generi les claus d'accés, es podrien programar aquestes al dispositiu final mitjançant comandes AT, un fet que no ens ocuparà en aquest projecte.

5.2.5. Programació mitjançant comandes AT

Per tal de programar o variar configuracions del sensor es poden utilitzar comandes AT a través d'una eina de comunicació mitjançant port sèrie, com pot ser el programa PuTTY. Aquest procés es durà a terme mitjançant el cable de connexió entre dispositiu i usb.

Per defecte les comandes AT estan desactivades, per aquest motiu serà necessari introduir la contrasenya per defecte 123456 i aquestes s'activaran durant 5 minuts. Pel fet que en aquest projecte no serà pràcticament necessària la manipulació de configuracions del sensor, s'utilitzaran les mínimes possibles. Totes les comandes disponibles les podrem trobar fàcilment a la guia del fabricant.



Figura 22: Cable de programació del sensor. [10]



Figura 23: Convertidor USB a TTL CH340G.

5.2.6. Especificacions del dispositiu

En la següent taula (Taula 8) es resumiran de forma general les principals característiques a tenir en compte del dispositiu que incorporarà els tres sensors que utilitzarem.

Protocol	Clase A LoRaWAN.
Bandes de freqüències	CN470, EU433, KR920, US915, EU868, AS923, AU915.
Configuració remota	Disponible a través de l'enllaç descendent de LoRaWAN mitjançant comandes AT.
Actualitzacions firmware	A través del port del programa.
Bateria	2400mAh, aprox. 10anys.
Sensors	Temperatura i humitat.
Indicador d'estat	LED tricolor.
Registre de dades	3200 registres amb datetime.

Taula 8: Especificacions Dragino LHT65.

6. PROTOCOLS DE COMUNICACIÓ

Els primers equips o dispositius creats tenien la capacitat de realitzar determinats procediments específics que solien ser propis de cada fabricant en termes de comunicació entre ells, aquests mètodes de comunicació han anat augmentant a mesura que ha augmentat el desenvolupament de dispositius o inclús s'han millorat molts dels protocols inicials, establint però sistemes de comunicació generals o fent-los Open Source permetent així la comunicació entre tot tipus de dispositius independentment de quin fabricant pertanyin. Per tal de realitzar aquestes connexions hi ha una gran quantitat de protocols de comunicació que estableixen un conjunt de normes per a cadascun.

En aquest apartat tractarem els protocols de comunicació que seran objecte d'estudi en aquest projecte, aquests protocols de comunicació que s'estudiaran vindran determinats per les possibilitats de comunicació del Node-RED de la nostra gateway (Fig. 24), alhora també de la capacitat de WinCC OA per a utilitzar-los, tot i que aquest últim té disponibilitat per a un gran nombre d'aquests. Entre els protocols de Node-RED i degut a la finalitat d'aquest projecte s'estudiaran TCP/IP, UDP, MQTT. Per altra banda també s'estudiarà la possibilitat d'implementar OPC UA i la relació de Modbus amb TCP/IP.

Abans de detallar cadascun dels protocols és molt important detallar que TCP/IP per si sol ja és un protocol, i que OPC UA i MQTT, entre altres, el que fan és utilitzar aquest protocol en el seu funcionament.

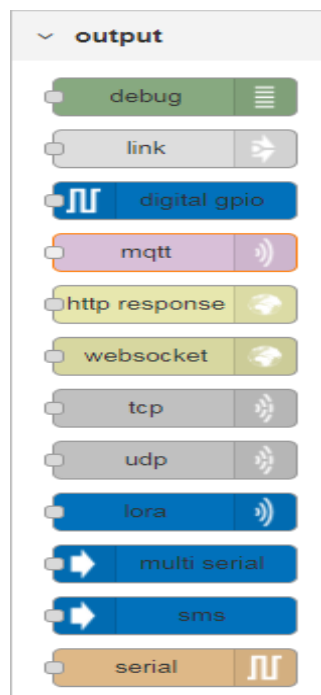


Figura 24: Protocols de comunicació disponibles a la gateway.

6.1. TCP/IP

El model TCP/IP sorgeix l'any 1969 per a projectes de defensa de EE.UU. i és la unió d'aquests dos protocols de xarxa el que permet la comunicació entre dispositius que pertanyen a la mateixa, i que resulta fonamental entendre per treballar en aspectes relacionats amb xarxes tal com ho és per a les persones poder parlar un llenguatge comú. En l'actualitat ja adoptat com a protocol estàndard d'Internet la gran majoria de dispositius connectats a una xarxa utilitzen aquest model TCP/IP que permet un intercanvi de dades i/o informació fiable i precís dins una xarxa mitjançant l'assignació d'una adreça única en tota la xarxa a cada equip connectat a aquesta.

EL software d'aquest protocol de comunicacions resulta complex, ja que es tracta de dos protocols de xarxa que operen a diferents nivells de capes i esdevé necessari unir diferents procediments per establir un intercanvi de dades fiable però estandarditzat. Aquests procediments s'agrupen en models de capes jeràrquiques, on cada capa es construeix sobre l'anterior sol·licitant-li serveis per poder donar resposta a la capa següent. Tot i que TCP/IP no correspon directament al model OSI ja que és anterior, es basa en aquest combinant diverses capes OSI en una única o no utilitzant-ne algunes per dividir els processos de comunicació, tal com es mostra a la taula següent (TAULA 9). Així doncs, les dades passen per aquestes quatre capes independents abans de rebre's a l'altre extrem i es recorren inversament una vegada les dades han arribat a l'extrem per tal de recodificar les dades per al destinatari.

TCP/IP	OSI	Exemples de protocols tcp/ip
Capa 4 o d'aplicació: Defineix els protocols de les aplicacions de xarxa que es comuniquen amb la capa de transport per enviar i rebre dades.	7. Aplicació	Serveis TCP/IP com ftp, tftp, i telnet.
	6. Presentació	
	5. Sessió	Altres com http, NFS, NIS, DNS, LDAP, rlogin, rsh, rcp, RIP, RDISC, SNMP.
Capa 3 o de transport: Utilitza els ports per a que les aplicacions puguin intercanviar informació entre dos punts, també permet conèixer l'estat de la transmissió de dades i garanteix que els paquets arribin sense errors i en seqüència.	4. Transport	TCP, UDP, SCTP.
Capa 2 o d'internet: Considerada la capa més important engloba diferents protocols on IP és el més important i identifica el tipus pel paquet de dades, s'encarrega de controlar la	3. Xarxa	IPv4, IPv6, ICMP mitjançant routers i gateway.

comunicació entre equips elegint la ruta més adequada que han de seguir els paquets anomenats datagrames per arribar a destí.		
Capa 1 o d'accés a la xarxa: Possibilita l'accés físic dels equips connectats a la xarxa especificant les característiques del hardware que s'utilitzarà per a aquesta.	2. Enllaç de dades	
	1. Física	ARP, Ethernet (IEEE 802.3), RS-232, IEEE 802.2

Taula 9: Equivalència entre les capes TCP i OSI.

IP significa Internet Protocol i s'encarrega de proporcionar a cada equip connectat a la xarxa la direcció anomenada amb el mateix nom formada per quatre octets decimals, per exemple 192.168.104.242, per enviar dades a altres màquines de la xarxa, és a dir realitzar el transport de dades punt a punt seleccionant la millor ruta. Aquests equips poden ser hosts clients, servidors o inclús els propis encaminadors.

L'enviament de dades es realitza mitjançant datagrames, que són paquets IP en aquest protocol no orientat a connexió ja que l'intercanvi de dades entre emissor i receptor es pot fer sense acord previ i un paquet pot seguir una ruta completament diferent a un altre en ser tractats de forma independent, així doncs el paquet de dades buscarà el camí més ràpid per arribar a la xarxa ja que segons la topologia de xarxa ens trobarem amb més o menys encaminadors com pot ser un passar o no per un switch.

Per altra banda no implementa correcció d'errors ni verificacions d'entrega de datagrames, ja que aquests controls formaran part de TCP.

TCP significa Transmission Control Protocol i és un dels protocols fundacionals d'Internet orientat a la connexió de IP's, pertany al nivell de transport i permet establir la connexió i intercanvi de dades entre dos dispositius host proporcionant un transport fiable de dades amb control d'errors que asseguri l'arribada i l'ordre dels paquets a destí, transmetent caràcter per caràcter per augmentar la seguretat enfront a problemes en lloc de per paquets discrets sencers de la següent forma:

- Punt de partida on el host d'origen estableix connexió amb el host de destí.
- Transmissió completa en ordre de bytes.
- Punt final que tanca la connexió del host d'origen i el de destí.

Per tal d'aclarir aquests conceptes podem pensar en la següent similitud, la direcció IP representa un nº de telèfon, mentre que TCP és la tecnologia que permet al telèfon rebre o emetre trucades. Per tant podem observar com aquests protocols no tenen especial ús si pensem en utilitzar-los per separat.

6.2. UDP

El protocol UDP utilitza la mateixa capa que el protocol TCP, la capa de transport, però la diferència entre aquests és que UDP no està orientat a connexió, això significa que en aquest protocol emissor i receptor no necessiten establir una connexió prèvia entre ells per a l'intercanvi de dades, per tant UDP no assegura un transport de datagrames fiable entre dos punts ja que no realitza cap tipus de verificació de connexió o errors, un fet que repercuteix però en una major velocitat de traspàs de datagrames i evita interrupcions per reenviar paquets perduts utilitzat en enviaments multicast, broadcast o transmissions a temps real on s'envia informació a molts hosts al mateix temps i es vol evitar la complexitat de cadascun d'aquests hosts, sacrificant la pèrdua de parts d'informació per garantir l'emissió en temps real.

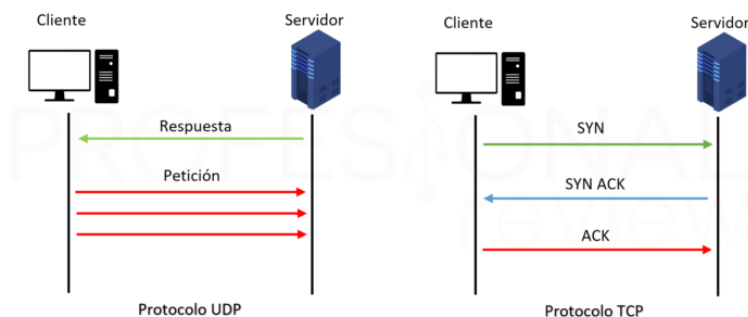


Figura 25: Diferència entre UDP i TCP. [11]

6.3. MODBUS

Modbus és un protocol de comunicació que utilitza el bus sèrie o port utilitzat per a la comunicació de dispositius electrònics a nivell industrial, especialment dispositius d'automatització i de camp com PLC cap a controladors principals o sistemes de recol·lecció de dades SCADA o similar, és un dels protocols més utilitzats a dia d'avui i des de finals dels anys 70. La seva estructura segueix el model Mestre/Esclau o Client/Servidor i és independent de la tecnologia i del fabricant ja que no disposa de patents. És un protocol d'aplicació que pot implementar-se en diferents capes de la capa física equivalent al model OSI. Aquest protocol pot operar en diferents modes de transmissió de dades, que són els següents:

- **Modbus TCP:** Comunicació ETHERNET TCP/IP basada en un model client/servidor on l'únic requisit és que els nodes es trobin en el mateix interval de adreces IP. Aquest protocol permet a equips industrials i altres dispositius similars connectar-se sobre una xarxa ethernet.
- **Modbus RTU:** Transmissió a través de RS-232 o RS-485 a una unitat remota RTU, per tant caldrà tenir en compte els paràmetres de comunicació com baudrate, paritat i bit de parada. Aquesta opció és útil per a comunicacions sense fil i la utilitzen fabricants ja que ho poden incorporar als seus productes sense càrrecs.

- Modbus ASCII: És la implementació més antiga que conté tots els elements de RTU però amb format de caràcters ASCII hexadecimal de 4 bits cadascun. Actualment és considerat un protocol obsolet.

El seu funcionament es basa en el fet que l'aplicació accedeix a modbus pel port 502, per defecte, en la pila TCP/IP. A continuació a modbus es genera una sol·licitud per part del client i el servidor respon.

Un dels factors importants a l'hora de treballar en IoT i la indústria 4.0 és la seguretat, un punt on Modbus és inferior a altres protocols com OPC UA ja que en l'època que es va desenvolupar els virus i ciberatacs no representaven una amenaça. És per aquest motiu que en l'actualitat ja es disposa d'adaptacions de modbus sobre OPC UA.

6.4. MQTT

MQTT significa Message Queue Telemetry Transport i sorgeix l'any 1999, és un protocol open source "machine to machine" (M2M) molt utilitzat en la IoT degut a la seva senzillesa basada en TCP/IP útil per aplicacions on s'envien quantitats petites d'informació.

El funcionament d'aquest protocol es basa en un servei de missatgeria client-servidor, basat en publicador i subscriptor comunicats a través d'un servidor central anomenat broker, transmetent la informació mitjançant una cadena payload amb estructura jeràrquica d'arbre delimitada amb la comanda "/", similar a un directori de carpetes i que serveix alhora per definir bé les especificacions del missatge. Les parts implicades en aquest procés són les següents:

- Broker: Servidor central que distribueix i filtra la informació segons un Topic o tema. Degut a aquest el que publica la informació no necessita saber res del node que rebrà aquesta, a més a més tot i que la comunicació d'informació acostuma a ser a temps real, el broker té la capacitat d'emmagatzemar missatges per a clients que no estan disponibles en un cert instant.
- Topic: Nom del missatge que serveix com a identificador d'aquest i on s'hi subscriuran els clients.
- Publicador: Client que envia la informació al broker per distribuir-la als clients subscrits a aquesta.
- Subscriptor: Clients que es subscriuen a un tòpic i rebran la informació d'aquest per part del broker.

- Client: El client pot ser tant un publicador com un subscriptor, rebent informació del medi o executant alguna funció d'interacció.

Així doncs el procés es divideix en quatre etapes que són connexió, autenticació, comunicació i finalització. El client inicia una connexió amb el broker per TCP/IP, per defecte al port 1883, i li envia un missatge per a la connexió que és respost per part d'aquest últim. Una vegada establerta la connexió el client publica els missatges amb el topic i payload, que representen el tema i la informació. Per altra banda el subscriptor també s'ha de connectar amb el broker i subscriure's al tòpic que voldrà rebre, podem disposar de múltiples clients a un topic.

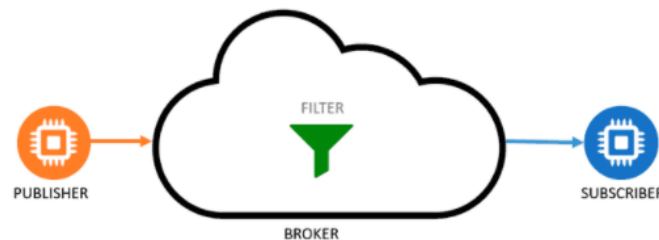


Figura 26: Arquitectura del protocol MQTT. [12]

Per altra banda MQTT disposa de QoS, Quality of Service, una característica que variarà segons les necessitats del sistema i que defineix la qualitat del servei en tres nivells:

1. QoS = 0: El missatge només s'envia una vegada, existeix la possibilitat de pèrdua d'un missatge i aquest no es tindrà en compte.
2. QoS = 1: El missatge s'envia fins que es garanteix l'entrega existint la possibilitat de rebre algun missatge duplicat.
3. QoS = 2: El missatge arribarà només una vegada per tal d'evitar duplicitats per evitar per exemple cobraments dobles en un sistema de pagament.

En termes de seguretat MQTT disposa de diferents mesures per protegir les comunicacions, com és la comunicació SSL/TLS i l'autenticació per usuari i contrasenya o mitjançant certificat, que necessita menys recursos.

6.5. OPC UA

OPC significa Open Protocol Communication i va sorgir a mitjans dels anys noranta per donar solució a la problemàtica que existia a les plantes industrials degut al gran nombre de drivers i protocols de comunicació diferents que existien segons el fabricant, fet que dificultava les instal·lacions i l'adherència de noves màquines al sistema. Aquest es fonamentava principalment en dues tecnologies, en primer lloc l'arquitectura client-servidor on es necessiten dos softwares independents, un servidor per tractar les dades i un client que faci les

consultes pertinents. En segon lloc la tecnologia COM/DCOM basada en Windows. Especialment aquesta segona tecnologia ha evolucionat juntament amb la seguretat en la següent versió anomenada OPC UA.

OPC UA (Unified Architecture) és una tecnologia de comunicació industrial basada en client i servidor evolucionada de la OPC Clàssica de la mà de OPC Foundation, aquest protocol de comunicació està pensat per comunicar dades d'equips industrials essent multiplataforma i orientat a serveis, tot d'una forma més segura que la tecnologia inicial degut a l'encriptació. Tot i que igual que la tecnologia anterior és molt útil per sistemes empresarials i monitoratges, la principal diferència amb la OPC Clàssica és que aquesta evolució no està només encarada a comunicació de dades entre aplicacions SCADA i sensors, sinó que pot comunicar dades de màquines a qualsevol aplicació degut a que disposa de millors tecnologies i models de dades. Així doncs la finalitat de OPC UA és enviar dades o conjunts de dades d'una forma fiable, segura i sobretot senzilla per tal que aquestes puguin estar disponibles a qualsevol aplicació o dispositiu client.

OPC UA és el protocol més destacat de la indústria 4.0 i està pensat per a ser segur, ja que implementa seguretat a tres nivells diferents per a l'autenticació, la firma i encriptació i l'ús de certificats digitals.

7. DISSENY DE LA SOLUCIÓ

7.1. Diagrama de la instal·lació

Prèviament a detallar el resultat final d'aquest projecte es mostra el diagrama i estructura final d'aquesta, on es poden observar els diferents elements detallats anteriorment juntament amb la seva funcionalitat. Tal com s'esmenta en l'apartat introductori el transcurs d'aquest projecte ha estat desenvolupar una idea inicial resolent les dificultats o millores que es poguessin aportar en aquest, en aquest sentit ens trobarem amb InfluxDB i Grafana que han estat útils per simplificar el sistema, tot i que contradictòriament poden semblar una càrrega no necessària en aquest.

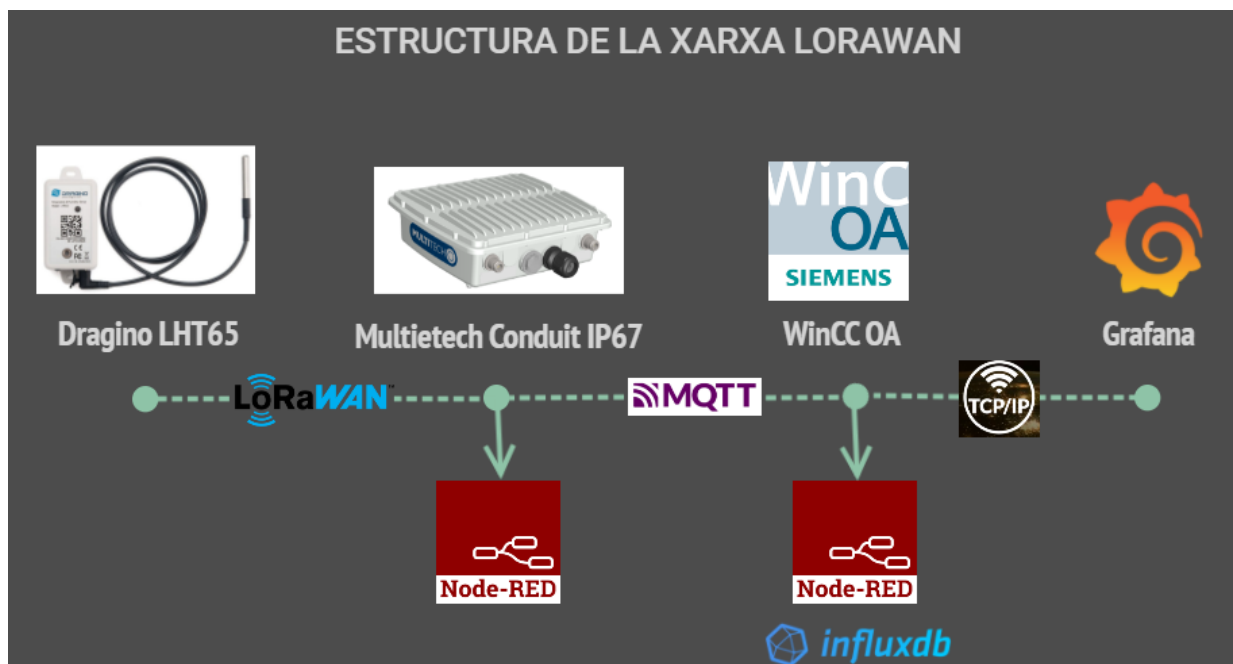


Figura 27: Diagrama de la instal·lació.

7.2. Gateway

Tot i que la tecnologia LoRaWAN utilitza majoritàriament passarel·les que envii la informació a un servidor extern encarregat de fer el tractament de les dades, en aquest projecte es va prendre la decisió d'utilitzar el model Multitech Conduit IP67, de caire més professional el qual té la possibilitat de realitzar la funció de servidor. Aquestes característiques entre altres fan que les opcions de configuració i gestió de la gateway siguin molt més completes respecte a altres, un fet que ha dut a dedicar-hi una gran part de les hores destinades al projecte degut a la gran quantitat de nous conceptes fins ara desconeguts i relacionats en l'àmbit de telecomunicació i informàtica, així com la necessitat d'autoaprenentatge, recerca i nombroses proves de funcionament.

7.2.1. Configuració

A continuació es descriurà el conjunt de la configuració de la gateway per tal que aquesta realitzi les funcions desitjades. Degut a que el menú de configuració (Fig. 28) d'aquesta consta

d'un conjunt nombrós d'apartats i subapartats i per tal d'explicar la configuració d'una forma clara i entenedora, es realitzarà una explicació seguint l'ordre de cadascun d'aquests, fent èmfasi als que realment afectin la funcionalitat del dispositiu pel que fa a la necessitat d'aquest projecte. Per altra banda, en A) i B) de l'annex d'aquest document es detallaran la resta de seccions que no afecten aquest projecte de forma directa, així com imatges de les diferents pestanyes de configuració respectivament.

Home	LoRaWAN ®	Setup	SMS	Administration	Commands
Save and Apply	Network Settings	Network Interfaces	SMS Configuration	User Accounts	Save Changes
LoRaWAN ®	Key Management	WAN Configuration	Send SMS	Self-Diagnostics (beta)	Revert Changes
Setup	Gateways	Global DNS	Received	Access Configuration	Restart Device
Cellular	Devices	DDNS Configuration	Sent	RADIUS Configuration	Save And Apply
Firewall	Device Groups	DHCP Configuration	Tunnels	X.509 Certificate	Restart LoRa Services
SMS	Profiles	GPS Configuration	GRE Tunnels	X.509 CA Certificates	Apps
Tunnels	Packets	SMTP Configuration	IPSec Tunnels	Remote Management	
Administration	Downlink Queue	SNMP Configuration	OpenVPN Tunnels	Notifications	
Status & Logs	Operations	Time Configuration	Status & Logs	Web UI Customization	
Commands	Cellular	Firewall	Statistics	Firmware Upgrade	
Apps	Cellular Configuration	Settings	Services	Save/Restore	
Help	Wake Up On Call	Trusted IP	Mail Log	Debug Options	
	Radio Status	Static Routes	Mail Queue	Usage Policy	
			Notifications Sent	Support	

Figura 28: Seccions de configuració Multitech Conduit IP67.

- LoRaWAN

LoRaWAN és la secció més important pel que respecta a la configuració de la xarxa a implantar ja que és en aquest on es detallaran pràcticament totes les característiques d'aquesta.

En primer lloc ens trobarem amb **Network Settings** on configurarem la funcionalitat de la nostra xarxa entre *Network Server* o *Packet Forwarder* i on podrem observar l'estat d'un o altre servidor, és a dir si està funcionant, parat o desactivat en el mode corresponent. Degut a que en el nostre cas realitzarem el tractament de les dades al propi servidor de la gateway, el mode de funcionament escollit i en el que ens centrarem és el primer, *Network Server*. Pel que fa al mode *Packet Forwarder* aquest s'utilitza per reenviar els paquets de dades a un altre servidor extern, com podrien ser els de chirpstack, The Things Network o un propi de l'usuari.

Una vegada amb el mode de funcionament escollit disposarem d'altres ajustaments, alguns d'aquests es generaran automàticament i altres seran decisió de l'usuari, com seran el canal de freqüència desitjat, que serà el de 868MHz a Europa i el mode de xarxa que podrà ser públic o privat depenent si volem crear una xarxa amb un servidor central o volem utilitzar la gateway com a únic servidor. Finalment trobarem altres característiques relacionades amb telecomunicacions i configurades per defecte les quals no s'entraran en detall.

A continuació trobem la secció on gestionarem els nostres nodes finals, **Key Management**. Existeixen dues possibilitats per a fer aquesta gestió, utilitzant el núvol o claus locals. En el nostre cas s'afegiran de forma manual els dispositius amb les seves claus OTAA o ABP corresponents. Finalment pel que fa a Class i Network Profile faran referència a 2.1.3.1. on seleccionarem la classe de comunicació dels nostres dispositius entre A, B o C. Cal esmentar però, que en un futur caldrà estudiar un mètode per realitzar un registre de nodes finals d'una forma més automatitzada, la qual cosa podrà arribar a implicar la utilització del núvol que es pretenia evitar en aquest projecte.

A **Gateways** i **Devices** podrem trobar informació dels paquets de dades rebuts i enviats i informació dels sensors connectats a la xarxa respectivament. Pel que fa a **Device Groups** aquest serveix per agrupar dispositius i realitzar actualitzacions o enviar missatges C2D, Cloud to Device de forma massiva a tots els dispositius del grup, un element que no podrem utilitzar ja que implica el Cloud.

Finalment l'última secció de LoRaWAN a tenir en compte és **Packets**, en aquesta trobarem el registre dels paquets de dades rebuts i enviats així com les peticions per connectar-se a la xarxa i el resultat d'aquestes dels diferents nodes finals, també el nivell de senyal RSSI amb què arriben les dades de cada sensor entre altres, un apartat molt útil quan encara no es disposa d'un mitjà de consulta o representació de les dades.

- Setup

En aquest apartat i concretament a **Network Interfaces** realitzarem la configuració d'interfície de la xarxa, és a dir mitjançant eth0 configurarem la direcció de la nostra gateway. En el cas d'aquest projecte se li ha configurat una IP estàtica 192.168.171.94, amb la seva màscara, gateway i DNS corresponents a la xarxa de bonArea. Per altra banda, tot i que no es tindran en compte es podran configurar el pont de xarxa br0 o el protocol punt a punt ppp0.

Altres opcions com **DDNS, DHCP o GPS Configuration** no es tindran en compte, ja que són complements no necessaris per al moment i les funcions bàsiques estan configurades per defecte.

- Administration

En aquesta secció ens centrarem en **Access Configuration**. En aquesta detallarem les opcions d'accés HTTP i HTTPS al servidor web, els protocols SSH i ICMP i a l'aplicació Node-RED entre altres.

Per altra banda seran també interessants els subapartats Web UI Customization, Firmware Upgrade i Save/Restore, on podem adaptar la interfície web a escala visual, actualitzar el firmware de la gateway o carregar, guardar configuracions respectivament.

7.2.2. Node-RED en Multitech Conduit

7.2.2.1. Explicació general

El fet d'utilitzar una gateway que alhora actues com a servidor i que incorpores Node-RED per realitzar el tractament de les dades d'una forma més senzilla que la programació tradicional era un avantatge considerable a l'hora d'aplicar un sistema d'aquestes característiques a la indústria, per tal de principalment facilitar el manteniment i la comprensió de la instal·lació a operaris que no estiguin familiaritzats en aquest àmbit. Durant el transcurs del projecte i una vegada es va iniciar el tractament de dades amb Node-RED es va detectar una limitació no prevista en aquest, i és que degut a una limitació en la memòria d'emmagatzematge el Node-RED que incorpora la gateway no permet la instal·lació de nodes extra a banda dels instal·lats per defecte, la qual cosa limitava algunes opcions o aplicacions que s'hi volien dur a terme, especialment en termes de protocols de comunicació i gestió d'avisos. Degut a que WinCC OA disposa de Node-RED aquest no ha resultat ser un factor d'elevada importància, però si cal tenir en compte en futures instal·lacions que segons la finalitat del projecte serà necessària una altra plataforma Node-RED on si es puguin instal·lar els nodes necessaris que veurem a 7.3.1, com seran els pertanyents al broker MQTT, Influx DB i Telegram en el cas d'aquest.

7.2.2.2. Nodes configurats i programats

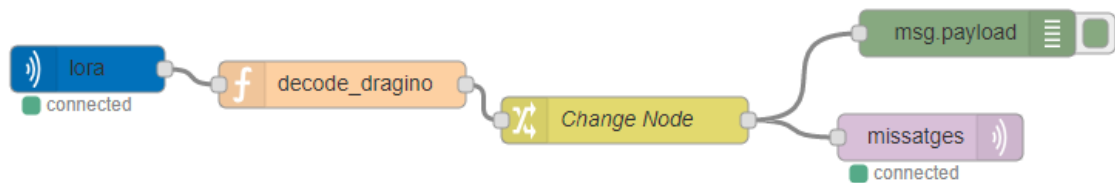


Figura 29: Node-RED del servidor en la gateway.

Lora:

Aquest serà el Node encarregat d'extreure el missatge hexadecimal de la gateway i és a partir del qual podrem extreure la informació per fer-ne el posterior tractament. No és necessari introduir-li cap tipus de configuració ja que està directament relacionat a la gateway i la seva funció és molt concreta. En les següents figures podem observar un exemple de les dades que es reben seleccionant entre observar el missatge complet (Fig. 30) o només el seu payload (Fig. 31).

```
msg : Object
{ "tmst": 1396014788, "chan": 3, "rfch": 1, "freq": 867.1, "stat": 1, "modu": "LORA", "datr": "SF9BW125", "codr": "4/5", "lsnr": -1.2, "rssi": -115, "opts": "", "size": 11, "fcnt": 810, "cls": 0, "port": 2, "mhdr": "40614f4400802a03", "appeui": "a8-40-41-7a-71-82-2e-08", "deveui": "a8-40-41-44-e1-82-2e-08", "ack": false, "adr": true, "gweui": "00-80-00-00-a0-00-5c-bd", "seqn": 810, "time": "2021-01-29T12:39:03.312209Z", "payload": [ 203, 207, 9, 12, 1, 185, 1, 8, 245, 127, 255 ], "eui": "a8-40-41-44-e1-82-2e-08", "_msgid": "da41533b.25beb" }
```

Figura 30: Objecte del missatge rebut.

```
msg.payload : buffer [11]
cbd308ce01b50108b77fff
```

Figura 31: Payload rebut.

Decode_dragino:

Decode_dragino és un node tipus funció que s'utilitza per descodificar el missatge hexadecimal rebut a la gateway per part del node final amb una funció creada per l'usuari. Cadascun dels 11 bytes del missatge hexadecimal que rebem pel node lora té el seu significat i tot i que els fabricants dels sensors acostumen a facilitar aquest codi a l'usuari, en aquest cas ha estat comprès en base a funcions exemple ja que en el cas dels Dragino LHT65 el fabricant només aporta aquesta funció per a les plataformes TTN i Chirpstack. A més a més d'aquesta descodificació del missatge provinent del node final s'adaptarà el missatge final a la necessitat d'aquest projecte, així doncs afegirem en aquests paràmetres que provenen de la gateway com són la data i hora, el DevEUI i la senyal RSSI.

FUNCIÓ IMPLEMENTADA PER A LA DESCODIFICACIÓ DEL MISSATGE

```
//S'inicia la variable datoHex que contindrà el missatge hexadecimal.
var datoHex = "";

//Analitzem la longitud del missatge i si no arriba a 16 caràcters afegim 0's, ho convertim a
string.
for (var i = 0, l = msg.payload.length; i < l; i++)
{
  if (msg.payload[i] <= 15)
  {
    datoHex = datoHex + "0" + msg.payload[i].toString(16);
  }
  else
    datoHex = datoHex + msg.payload[i].toString(16);
}

//Per a l'estat de bateria, temperatures i humitat es seleccionen els caràcters corresponents
del missatge hexadecimal i es parsejen per obtenir el seu valor en nombre real.
BAT_status = (parseInt(datoHex.substring(0, 4), 16) >> 14) & 0xFF; //Estat bateria
Built_In_Temperature = parseInt(datoHex.substring(4, 8), 16) / 100.0; //Temperatura interior
Built_In_Humidity = parseInt(datoHex.substring(8, 12), 16) / 10.0; //Humitat interior
Ext_value = parseInt(datoHex.substring(14, 18), 16) / 100.0; //Valor sensor extern

/*Resum de l'indicador de nivell de bateria.
00(b), 0: Ultra Low ( BAT <= 2.50v )
01(b), 1: Low ( 2.50v <=BAT <=2.55v )
10(b), 2: OK ( 2.55v <=BAT <=2.65v )
```

```

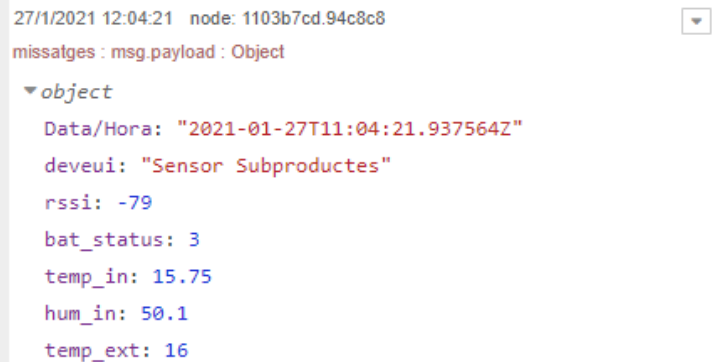
11(b), 3:Good (BAT >= 2.65v)
*/

//Creem i afegim les variables que volem mostrar al nostre missatge i generem la
estructura.
msg =
{
  "payload":
  {
    "Data/Hora": msg.time,
    "deveui":msg.deveui,
    "rssi":msg.rssi,
    "bat_status": BAT_status,
    "temp_in":Built_In_Temperature,
    "hum_in":Built_In_Humidity,
    "temp_ext":Ext_value
  }
};

return msg;

```

Taula 10: Funció implementada per a la descodificació del missatge.



```

27/1/2021 12:04:21 node: 1103b7cd.94c8c8
missatges : msg.payload : Object
  ▼ object
    Data/Hora: "2021-01-27T11:04:21.937564Z"
    deveui: "Sensor Subproductes"
    rssi: -79
    bat_status: 3
    temp_in: 15.75
    hum_in: 50.1
    temp_ext: 16

```

Figura 32: Format del missatge.

Change Node:

Ja que en el missatge rebut identifiquem cada sensor pel seu DevEUI corresponent, mitjançant aquest node canviarem la identificació del DevEUI per un nom que ens resulti més intuïtiu a l'hora d'identificar el sensor (Fig. 32). Aquest és el mètode més directe de realitzar aquest procés, tot i que posteriorment en l'apartat 9 se'n detallaran alternatives per xarxes amb un alt contingut de nodes associats.

Per realitzar-ho (Fig. 32) seleccionarem Change entre les opcions Set, Delete, Move i Change. A continuació detallarem quina part del missatge es vol canviar, msg.payload.deveui, introduïrem el corresponent al sensor que volem canviar el nom i finalment introduïrem el nom que volem establir.

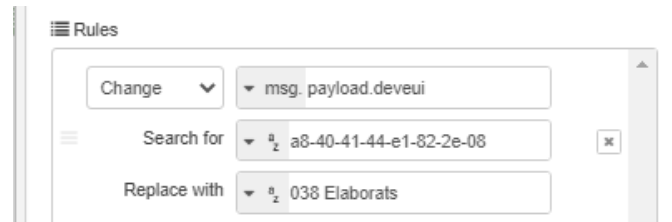


Figura 33: Vista del Change Node.

MQTT out:

Finalment MQTT ha estat el protocol escollit per realitzar la transmissió de dades a WinCC OA, tot i que existeixen altres mètodes aquest és el més testejat en termes de funcionalitat alhora que no genera canvis en l'estructura del missatge durant la seva transmissió, fet que ens facilitarà emmagatzemar els valors segons siguin temperatures, humitats o altres en la base de dades de la forma desitjada sense necessitat de noves adaptacions.

En primer lloc introduïrem el servidor i port on es volen enviar les dades, el qual disposarà del broker MQTT corresponent, a continuació introduïrem el nom del Topic que contindrà les dades i finalment seleccionarem la QoS desitjada, que serà de dos degut a que no ens interessa rebre un missatge duplicat però sí garantir-ne la seva arribada.

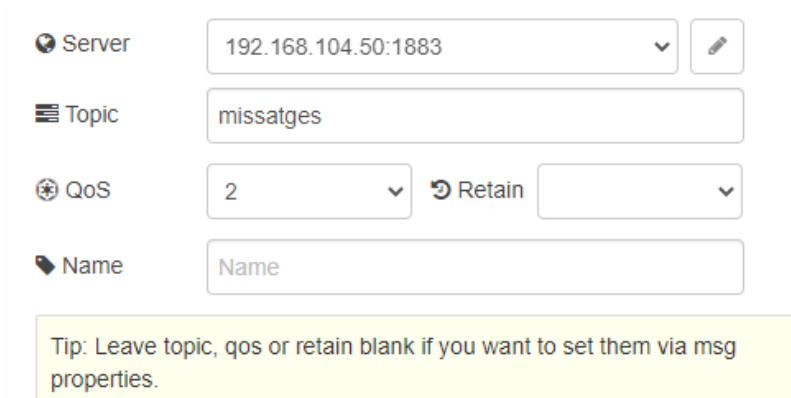


Figura 34: Configuració del node MQTT.

7.3. WinCC OA

Prèviament a iniciar-nos en el desenvolupament del procés realitzat a WinCC OA cal detallar la no utilització de la idea que es tenia inicialment en aquest. En un primer moment, i d'aquí l'èmfasi fet en els protocols de comunicació i el programa en si, es pretenia fer arribar les dades de la gateway directament a WinCC OA i emmagatzemar-ho en Datapoint, però durant el desenvolupament d'aquest i l'anàlisi de les opcions disponibles es va observar que aquesta idea no era òptima per al que es volia desenvolupar.

En primer lloc existien mancances en la comunicació entre gateway i WinCC OA, ja que a banda de la necessitat de llicències extra no quedava clara la forma de fer arribar les dades d'aquest en els drivers disponibles, o si bé calia crear-ne un. Com s'havia esmentat es tracta d'un software complex que en ocasions requereix força experiència per entendre'l i inclús usuaris avançats tenien dubtes de com dur a terme aquesta idea. En segon lloc la rebuda de dades provocava haver d'adaptar el missatge inicial al format amb què està configurat WinCC OA i els seus corresponents Datapoint, un fet que complicava en excés la identificació de les diferents variables que existeixen en aquest.

Així doncs amb la finalitat de facilitar el procés i a conseqüència el manteniment i comprensió es va decidir utilitzar l'eina Node-RED que WinCC OA incorpora i de la qual l'empresa té llicència, una eina que a més a més en cas que en un futur s'aprovi la utilització de WinCC OA permetria rebre el missatge d'una forma molt senzilla i guardar-lo en un Datapoint d'una forma molt més senzilla que mitjançant els drivers propis del programa.

7.3.1. Node-RED

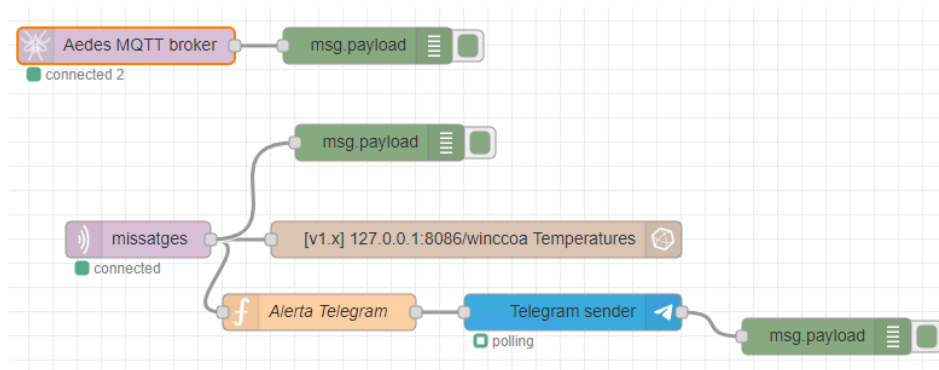


Figura 35: Node-RED en la aplicació de WinCC OA.

Aedes MQTT broker:

Un dels brokers MQTT més coneguts i utilitzats és Mosquitto, degut a que aquest l'hauríem d'utilitzar externament a Node-RED el broker Aedes és el que s'utilitza internament, aquest és el més recomanat en aquesta l'aplicació Node-RED. Únicament li haurem de configurar el port pel què tractarà les dades, acord amb els nodes MQTT in i MQTT out.

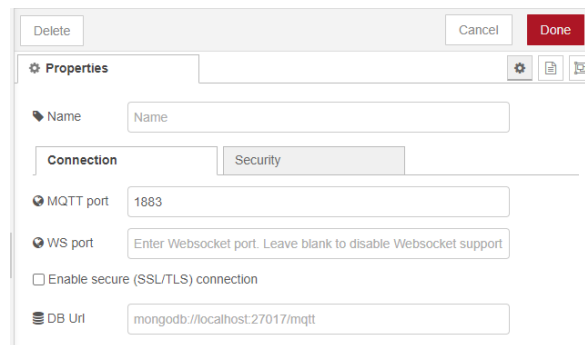


Figura 36: Configuració del node Aedes MQTT broker.

MQTT in:

Mitjançant aquest node rebrem les dades generades a la gateway, degut a que el protocol MQTT necessita un broker entre emissor i receptor aquest node rebrà les dades provinents del broker que les gestioni, Aedes MQTT broker en aquest cas. Necessitarem indicar-li el servidor on està allotjat el nostre broker, que serà en localhost en aquest cas, també el port que com s'ha detallat anteriorment serà el 1883.

Per altra banda tindrem l'opció d'indicar-li la QoS i el format del missatge de sortida, que seran 2 i *a parsed JSON object* respectivament. El primer és degut al fet que no interessa rebre un missatge duplicat pero si garantir-ne la arribada, mentre que el segon ens mostrarà el missatge amb el format desitjat per al seu posterior tractament.

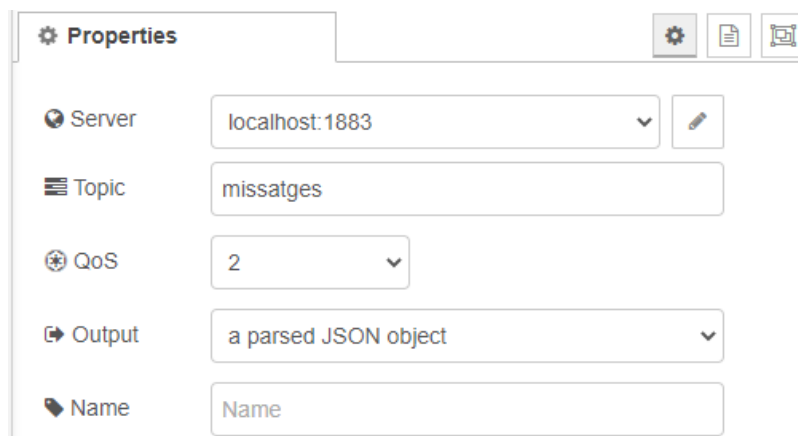


Figura 37: Node MQTT in.

InfluxDB:

Node on definirem la base de dades a la qual es desitgi emmagatzemar la informació rebuda prèviament. La base de dades no es crearà automàticament i en l'apartat següent es detallarà el procediment per crear-la dins l'estructura WinCC OA, ja que aquest node no la crearà per si sol. Caldrà configurar-li l'adreça del servidor on es troba allotjada aquesta base de dades, també el nom que la identifica i la seva mesura, que descriurà les variables

que s'emmagatzemen en aquesta. Així doncs a la següent imatge (Fig. 36) podem observar com utilitzem el servidor localhost i nomenem LoraWAN a la base de dades, on la seva mesura principal seran Temperatures.



Figura 38: Node Influxdb out.

Alerta Telegram:

En la funció d'aquest node funció es realitzarà un codi amb la finalitat d'enviar un missatge d'alerta mitjançant Telegram quan la temperatura d'un sensor superi un llindar de temperatura exterior prèviament establert. Aquest llindar s'establirà dins la mateixa funció i el missatge d'alerta contindrà l'identificador del node i un missatge informant del perill d'incendi.

FUNCIÓ D'ALARMA MITJANÇANT UN BOT DE TELEGRAM

```
//Si la temperatura exterior del sensor supera els 40 graus s'iniciarà la funció.
if (msg.payload.temp_ext >= 40) {

  //Afegim la variable missatge i n'especifiquem el text que contindrà amb les
  //variables corresponents dels valors del sistema que es vulguin mostrar.
  var my_message = 'ALERTA INCENDI! \nSENSOR: ' +
    msg.payload.deveui +
    '\nTEMPERATURA: ' +
    msg.payload.temp_ext + ' °C' +
    '\nDATA/HORA: ' +
    msg.payload["Data/Hora"]

  //Adaptem la sortida del missatge a la necessària per Telegram.
  msg.payload = {
    chatId: -408846150,
    type: "message",
    content: my_message
  }
  //Printem el missatge
  return msg;
}
```

Taula 11: Funció d'alarma mitjançant un bot de Telegram.

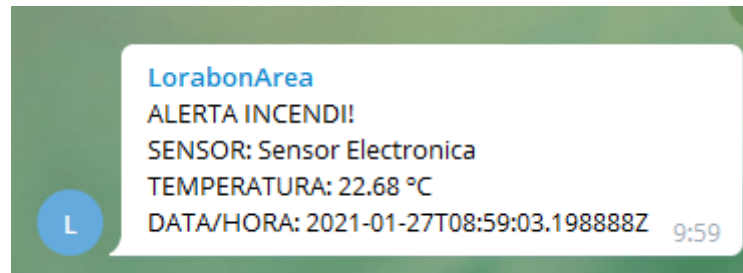


Figura 39: Missatge d'avís a Telegram.

Telegram Sender:

Mitjançant aquest node permetrem enviar l'avís personalitzat a la funció anterior mitjançant Telegram. Per tal de configurar aquest node prèviament necessitarem crear un bot, és a dir un usuari fictici que serà qui ens avisarà en el xat de l'alerta. Així doncs, una vegada amb el bot creat, caldrà indicar a la configuració del node el nom d'aquest bot, el seu Token identificador i el ChatID on s'enviarà el missatge.

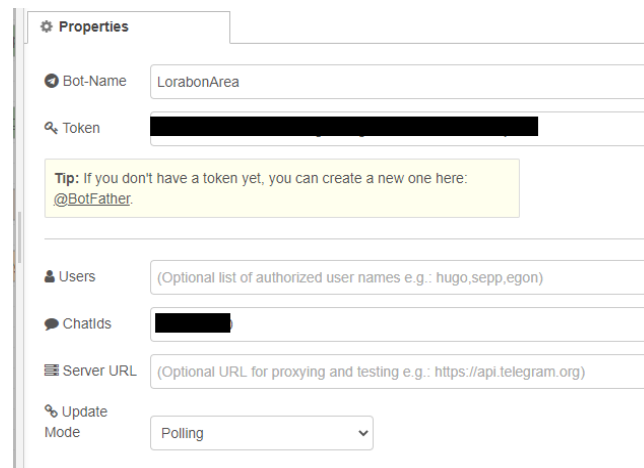


Figura 40: Node Telegram sender.

7.3.2. InfluxDB

InfluxDB és una eina incorporada dins l'estructura de WinCC OA i que podem utilitzar en el propi servidor d'aquest, de la mateixa forma que Node-RED. Aquesta eina s'utilitza per a l'emmagatzematge de les dades prèviament a la seva representació en una interfície visual, d'aquesta forma s'aporta un procediment més controlat i que segueix estàndards habituals en el tractament de dades i la forma d'accedir-hi des de la plataforma visual.

Per utilitzar aquesta eina WinCC OA incorpora el manager anomenat NextGen Archiver (NGA), que s'utilitza per al registre de dades d'operacions. Actualment aquest manager incorpora per defecte la base de dades de sèries temporals InfluxDB, en un futur Siemens donarà suport a altres tipus de bases de dades i versions actualitzades d'aquestes. Una vegada arranquem el

manager NGA a la consola de comandes WinCC OA iniciarà en segon pla la base de dades de InfluxDB. Per tal d'interactuar amb aquesta base de dades podrem iniciar un client d'influx a la nostra consola de comandes, on el llenguatge serà similar al SQL tot i que no es tracta d'una base de dades de tipus relacional.

Mitjançant una capa intermèdia WinCC OA s'encarrega de realitzar les consultes a la base de dades, sempre que aquesta estigui operativa. En cas contrari les dades s'emmagatzemaran en un buffer i quan la base de dades torni a estar operativa s'emmagatzemaran en aquesta (Store & Forward).

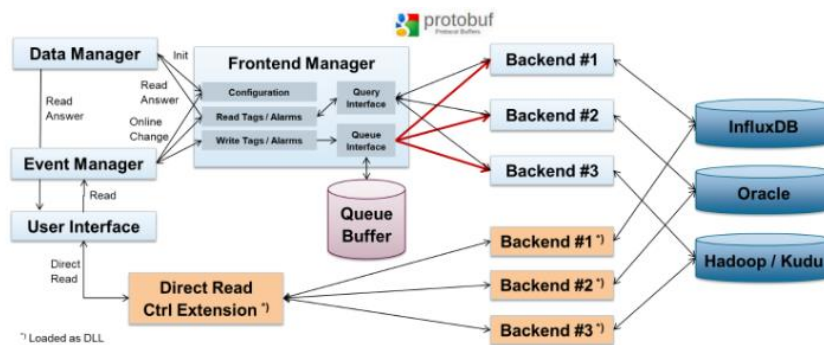


Figura 41: Arquitectura de NextGen Archive. [6]

Per tal de dur a terme aquesta operació serà necessària la realització de passos previs. En primer lloc mitjançant la consola de comandes es crearà la base de dades configurada al node corresponent a InfluxDB en Node-RED, ja que Influx no la crearà per si sol. Una vegada amb la base de dades creada i en funcionament les tasques que aquesta ha de realitzar es duran a terme automàticament, ja que des de Node-RED ja hem indicat que guardi les dades a la base de dades corresponent. Finalment, degut a que prèviament el missatge objecte ja ha estat dissenyat de forma que contingui el nom que identifica cadascuna de les dades i els seus valors corresponents, automàticament InfluxDB ja emmagatzemarà aquestes en la seva columna corresponent (Fig. 40).

```
> show databases
name: databases
name
----
winccoa
internal
LoraWAN
> use LoraWAN
Using database LoraWAN
> show measurements
name: measurements
name
----
Valors
> select * from Valors
name: Valors
time                Data/Hora                bat_status deveui                hum_in rssi temp_ext temp_in
-----
1611738261283976200 2021-01-27T09:04:21.742977Z 3                Sensor Subproductes 43.6  -80  14.93  14.67
1611739142725119900 2021-01-27T09:19:03.199377Z 3                Sensor Electronica  27.4  -114  22.81  23.07
>
```

Figura 42: Vista de la base de dades.

Finalment serà necessari crear la base de dades internament a WinCC OA ja que per defecte emmagatzema les dades a la base de dades per defecte wincoa. Per tal de crear una base de dades pròpia per al projecte que eviti conflictes de dades de diferents projectes i aporti seguretat en cas de corrompre's alguna d'aquestes, els passos realitzats són els que es detallen a continuació:

1. La configuració a modificar per a l'emmagatzematge de dades es troba a Backends, els quals depenen dels Profiles, que és on trobarem els diferents tipus de bases de dades tot i que actualment, com s'ha esmentat, l'única opció disponible és InfluxDB. Així doncs crearem un nou Backend.

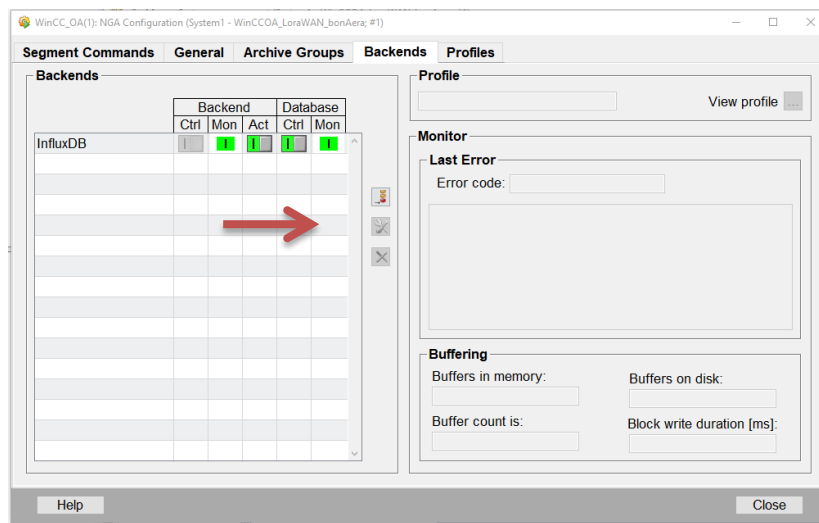


Figura 43: Creació del Backend.

2. El nom del Backend no tindrà relació amb el nom de la base de dades, però per conveniència en els projectes de l'empresa el nom d'aquest es farà coincidir amb el nom del projecte.

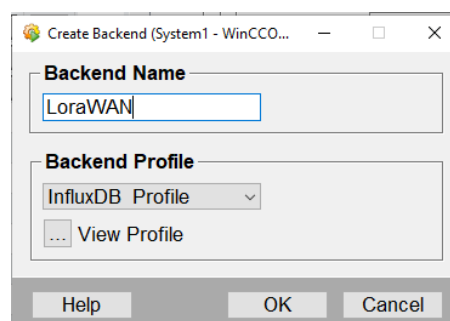


Figura 44: Nom del Backend.

3. Una vegada amb el Backend creat caldrà realitzar-ne la configuració modificant les pestanyes General i Database. A la pestanya General clicarem sobre el desplegable de l'apartat *Executable file* i seleccionarem l'única opció disponible, *NGAinfluxBackend*.

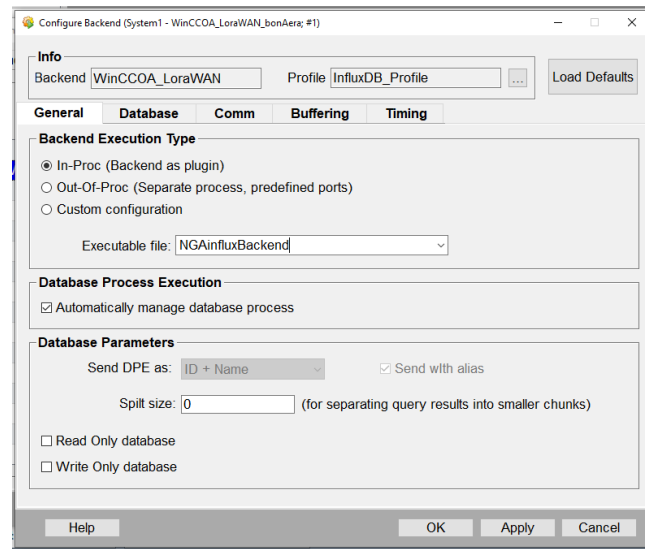


Figura 45: Configuració General del Backend.

Pel que fa a Database especificarem la IP i port del servidor de bases de dades InfluxDB, que serà localhost per defecte. A continuació especificarem el nom de la base de dades, usuari i contrasenya i el sistema de backup a DB Specific Configs fent click sobre la clau corresponent i escrivint el valor a la caixa de text on clicarem el tick verd posteriorment.

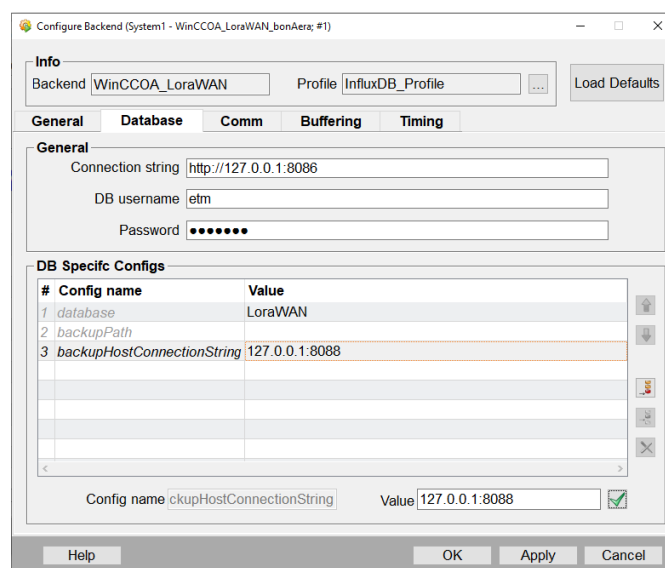


Figura 46: Configuració de la base de dades al Backend.

- Una vegada finalitzada la configuració del Backend modificarem la configuració dels Archive Group creant-ne un de nou. El nou Archive Group dependrà del Backend creat el qual seleccionarem al desplegable, a continuació i també per conveniència a l'empresa el nom del Archive Group serà el mateix que el del Backend i la base de dades. Per defecte l'Archive Group utilitzat a WinCC OA s'anomena EVENT i té una política de retenció de dades de 31 dies, un paràmetre que podrem ajustar segons convingui en el nostre cas.

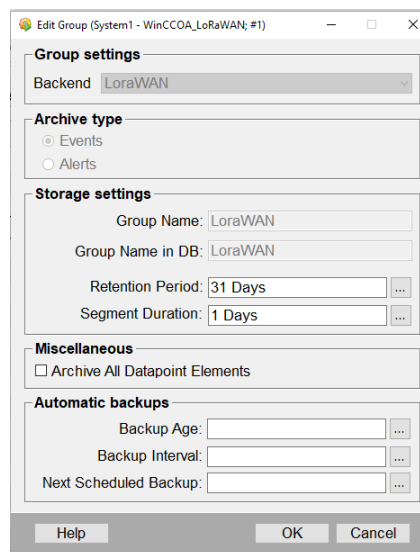


Figura 47: Creació del grup i política de retenció.

- Finalment i mode d'informació, si treballéssim mitjançant Datapoint utilitzaríem `config_archive` dins el mòdul PARA per indicar a WinCC OA que hauria d'utilitzar la configuració creada a Archive Group.

7.4. Grafana

7.4.1. Configuració

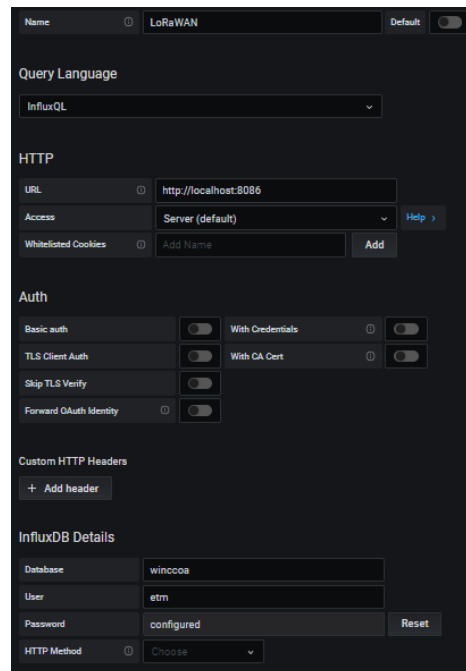
Mitjançant Grafana es realitzarà el monitoratge de les dades recopilades, aquesta és una eina molt útil i completa per a la representació gràfica. Els procediments realitzats per a la creació de la interfície visual han estat els següents:

- Afegir la base de dades:**

En primer lloc caldrà importar les dades corresponents a la base de dades on aquestes s'emmagatzemin, existeixen una gran quantitat d'opcions d'importació, des de Prometheus, Graphite o Elasticsearch fins a InfluxDB, que és la que ens ocupa en aquest projecte.

Una vegada seleccionem la importació des d'InfluxDB podrem configurar el nostre Data Source. En primer lloc introduïrem el nom desitjat a la nostra font de dades i a

continuació especificarem l'adreça URL on es troba la base que conté les nostres dades, finalment indicarem el nom de la base de dades a importar, juntament amb l'usuari i contrasenya si és que en té. Existeixen altres opcions de configuració més específiques, les quals no es té la necessitat d'utilitzar.



The screenshot shows the configuration page for a new data source named 'LoRaWAN'. The 'Query Language' is set to 'InfluxQL'. Under the 'HTTP' section, the 'URL' is 'http://localhost:8086', 'Access' is 'Server (default)', and 'Whitelisted Cookies' is empty. The 'Auth' section has 'Basic auth' and 'TLS Client Auth' disabled, 'Skip TLS Verify' disabled, and 'Forward OAuth Identity' disabled. The 'Custom HTTP Headers' section has an 'Add header' button. The 'InfluxDB Details' section has 'Database' set to 'winccoa', 'User' set to 'etm', 'Password' set to 'configured', and 'HTTP Method' set to 'Choose'. A 'Reset' button is next to the password field.

Figura 48: Creació del Data Source i importació de la base de dades.

2. Creació d'un dashboard:

Amb la font de dades definida es seguirà amb la creació d'un dashboard. Un dashboard no serà més que un panell de control on afegirem el conjunt dels nostres gràfics, existeix la possibilitat de crear carpetes d'aquests segons la seva finalitat.

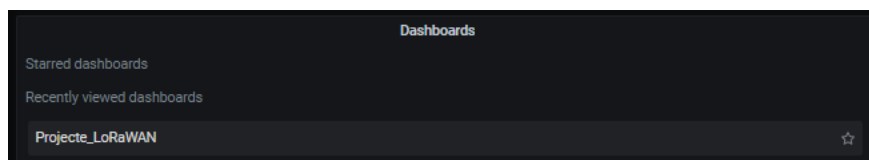


Figura 49: Dashboard del projecte.

3. Creació dels gràfics de representació:

Una vegada dins el nostre dashboard tindrem l'opció d'afegir els gràfics desitjats i entrarem en el panell de configuració d'aquests, on les opcions són múltiples.

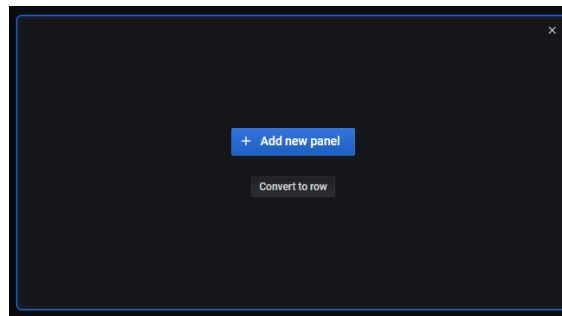


Figura 50: Creació d'una panell o gràfic.

En primer lloc seleccionarem el tipus de visualització gràfica desitjada, que pot ser gràfica, d'estats, de mesura, taula o text entre altres. En el cas d'aquest projecte s'utilitzen l'eina gràfica per a la representació de les temperatures i la humitat, també per a la representació pel nivell de senyal RSSI i finalment l'eina de mesura on es representa el nivell de bateria del sensor. Com s'observa a la següent imatge i per a les eines de visualització escollides existeixen un conjunt de paràmetres a configurar:

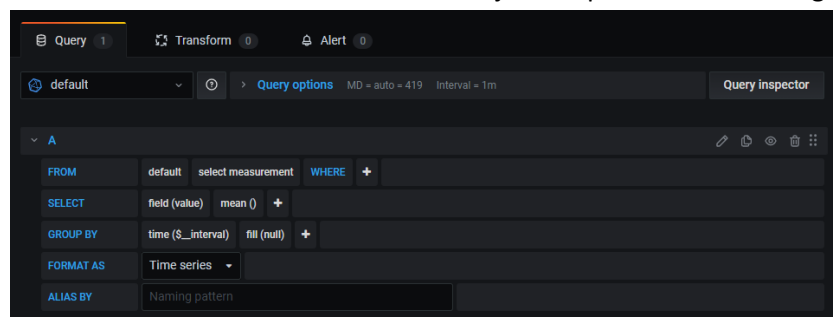


Figura 51: Panell de configuració de dades.

- Default: Espai on es definirà el Data Source d'on extreure les dades.
- Query A: Correspon al conjunt de configuracions d'una variable. És a dir, en A podrem configurar la representació d'una primera variable, mentre que si afegim una zona B hi podrem configurar una segona. Així doncs en el cas d'aquest projecte s'han utilitzat A, B i C per a Humitat, Temperatura Exterior i Temperatura interior respectivament. Existeix la possibilitat de representar tres variables en una mateixa Query, però en aquest cas impossibilita editar-ne una en concreta d'aquestes pel que respecta a color, grandària o format entre altres.
- FROM: En aquest apartat definim quin measurement volem extreure de la nostra base de dades, així com seleccionar si volem les dades només d'un sensor en concret.
- SELECT: Seleccionarem quina dada volem representar de les disponibles en el nostre measurement, així com si volem representar-ne el valor màxim, mínim o actual entre altres.

- **GROUP BY:** Indicarem en quin interval de temps volem agrupar les dades i com volem representar un valor no detectat. En aquest cas s'utilitza (\$__interval), una variable que ens deixarà modificar aquest temps segons escollim en la part superior dreta de la pantalla de representació del dashboard.

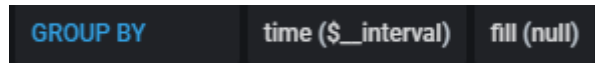


Figura 52: Eina GROUP BY.

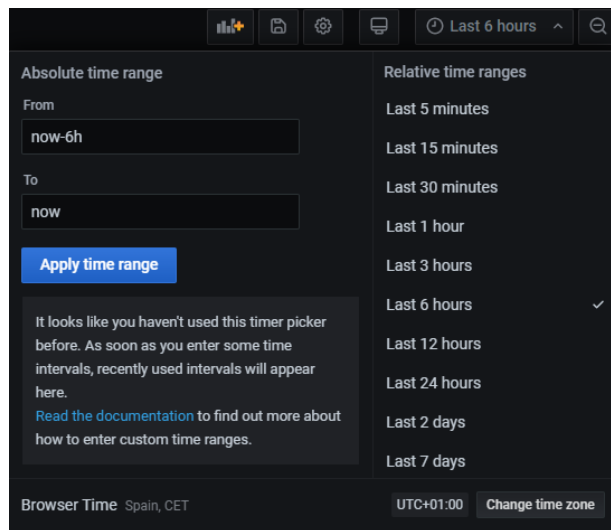


Figura 53: Desplegable per a la selecció del rang de temps de mostra.

- **FORMAT AS:** Seleccionarem el format de les dades entre Time series, Table o Logs. Com que representem sèries de dades temporals escollirem la primera opció.
- **ALIAS BY:** Espai on podrem identificar amb el nom desitjat la nostra variable, serà útil a l'hora de definir la nomenclatura que es visualitzi a la llegenda del gràfic.

4. Configuració visual del gràfic.

Finalment existirà la possibilitat de personalitzar la nostra gràfica a escala visual. Les possibles configuracions següents es mostren a la següent imatge (Fig. 53), d'on en destacarem els següents:

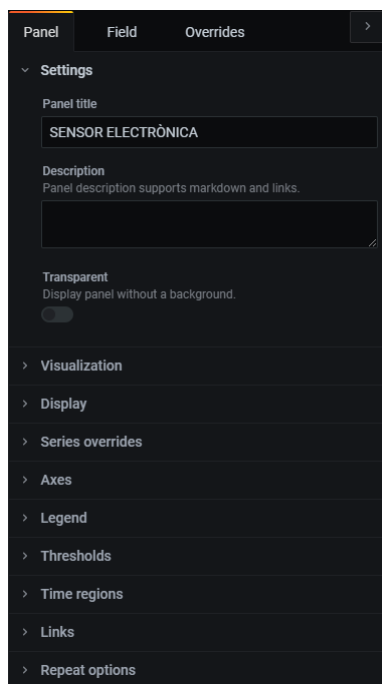


Figura 54: Configuracions visuals.

- Settings: Definirem el títol del nostre gràfic.
- Visualitzation: S'escull el model de representació anomenat anteriorment, en el nostre cas representació gràfica i de mesura.
- Display: Configurarem el gruix de la línia de representació així com si volem introduir punts en cada mesura, també si volem representar la línia d'alerta.
- Legend: S'afegirà la llegenda corresponent al gràfic així com els valors que es vulguin indicar, que seran el màxim, el mínim i l'actual.

5. Configuració del gràfic de mesures o gauge.

A banda de la configuració esmentada anteriorment el gràfic on representarem el nivell de bateria del sensor presenta una particularitat, i és que en aquest haurem de definir els seus rangs i que significa cadascun d'aquests. Així doncs, en l'apartat Field introduïrem el rang de 0 a 3, juntament amb un alert treshold a nivell 1 i el significat de cada valor. Per altra banda, si no arriben dades degut a algun problema s'indicarà No value! (Fig. 55).

NIVELL	DESCRIPCIÓ
0	Sense bateria
1	Bateria baixa
2	Bateria normal
3	Bateria alta

Taula 12: Nivells de bateria acord a la programació en el programa de descodificació del payload.



Figura 55: Indicador d'estat de bateria.



Figura 56: Indicador de falla en recepció de dades.

7.4.2. Eina alertes

Grafana disposa d'una eina per mostrar alertes en diferents plataformes en cas que es detectin valors fora d'un rang establert. En primer lloc caldrà dirigir-se a la zona Alerting i afegir un canal de notifikacions, que podrà ser via Email, Discord o Telegram entre múltiples opcions i que haurà de ser configurat segons les característiques de la plataforma escollida (Fig. 56). A continuació ens podrem dirigir al nostre gràfic corresponent el qual li vulguem afegir l'alerta, dirigint-nos a l'apartat de configuració Alert on indicarem el nostre canal de notifikacions i el tipus d'alerta que es desitgi juntament amb el missatge d'avís, per exemple que indiqui que el sensor s'està cremant quan aquest sobrepassa els 50 graus.

Després de realitzar un període de proves paral·lelament al mètode de Telegram programat a Node-RED, el corresponent a Grafana ha estat descartat. Tot i que visualment resultava molt útil i permet adjuntar la imatge corresponent a la gràfica en el moment de l'alerta, no és una eina que porti la precisió desitjada en aquest projecte, induint a errors en algunes ocasions a diferència de l'altre mitjà utilitzat.

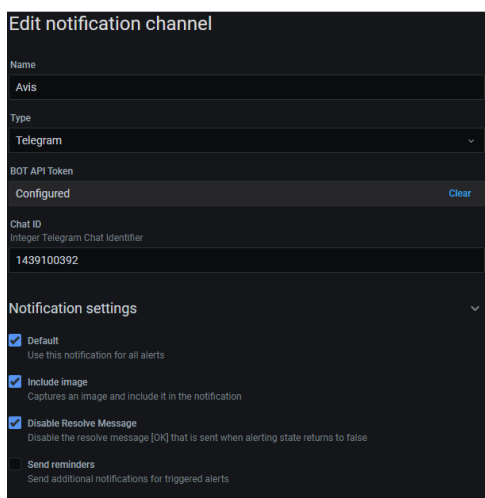


Figura 57: Creació d'un canal de notifikacions.

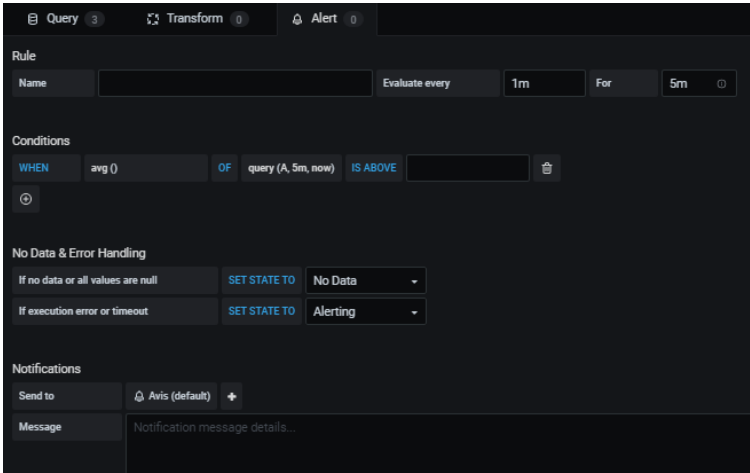


Figura 58: Configuració de la alerta.

7.4.3. Resultat final

A continuació s'observa el resultat final del monitoratge de dades d'un dels nodes finals operatius a la xarxa. En el gràfic principal podem observar la humitat i les temperatures interior i exterior del sensor. El fet de representar els dos valors de temperatura adopta la finalitat de comprovar que ambdós sensors del dispositiu funcionen correctament i capten temperatures similars, d'aquesta forma es detectaria ràpidament si algun dels dos no funcionen correctament.

A la part lateral podem observar el gràfic indicador de bateria, on es mostra entre Bateria alta, Bateria normal, Bateria baixa i Sense bateria segons l'escala de voltatges del sensor, descodificada en la funció de descodificació del missatge.

Finalment observarem el nivell de senyal RSSI del sensor corresponent, que ens serà útil per comprovar que aquest estigui situat en una zona correcta i detectar possibles interferències.

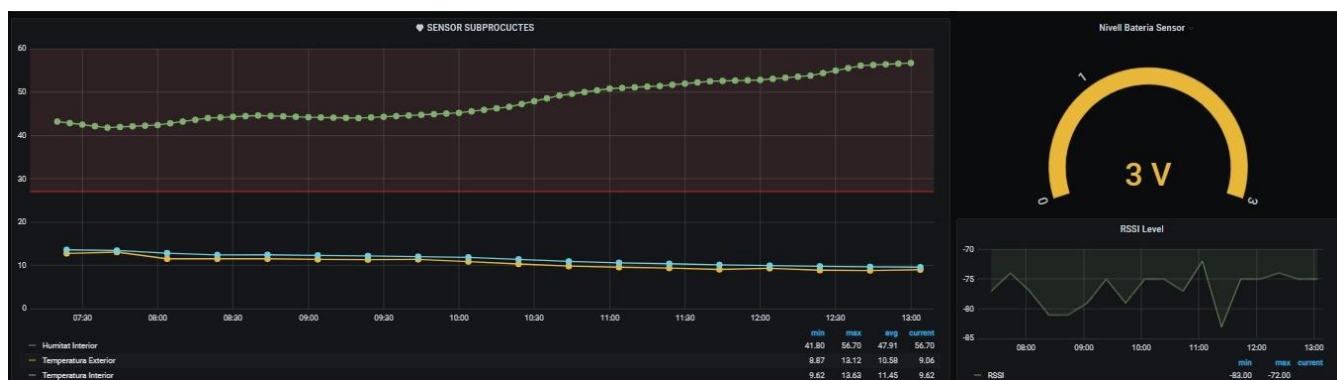


Figura 59: Monitorització de les dades.

7.5. Nodes finals: Dragino LHT65

Els dispositius sensors utilitzats en aquest projecte han estat 30 unitats de Dragino LHT65, és molt important abans de centrar-nos en el seu funcionament destacar la funcionalitat que aquests tenen en aquest projecte. Paral·lelament al desenvolupament de la xarxa LoRaWAN s'està desenvolupant un dispositiu sensor propi de bonÀrea, configurable mitjançant interfície web, el qual estarà preparat per adaptar-se a tot tipus de necessitats que hagin de ser capturades i que està en fase final per iniciar-se amb les proves. Així doncs, la finalitat de l'ús dels sensors Dragino LHT65 ha estat disposar de nodes finals per poder posar la xarxa en funcionament sense dependència de tercers, alhora que s'ha utilitzat com a referència i guia en alguns punts de desenvolupament del dispositiu propi, com és l'estructura del missatge original per a la seva posterior descodificació o la idea d'un mode alarma que força el missatge a partir d'una temperatura prèviament establerta.

Una vegada entesa la finalitat d'aquests en podem entendre els pocs canvis de configuració que s'hi ha realitzat en la mesura del possible, els quals es realitzen mitjançant comandes AT i que s'han realitzat amb el programa PuTTY ja utilitzat a l'empresa. Per altra banda es detalla també la no implantació d'una idea que segons el proveïdor ja estava en funcionament, però el fabricant va fer saber que no.

- Alarma en valor establert:

Segons el proveïdor en l'actual versió dels dispositius Dragino es disposava d'un mode anomenat Alarm Mode, aquest mode captava dades en períodes de temps molt curts i només enviava el missatge si es detectava un valor superior al rang que anteriorment se li havia programat com a límit, a banda de la transmissió durant el període prolongat de temps. Després de no poder assolir la programació d'aquest mode i contactar amb el fabricant, aquest va fer saber que Alarm Mode estaria disponible en la futura versió del dispositiu, però no en l'actual. Així doncs caldrà seguir l'evolució de la nova versió i si aquesta es pot implantar en els dispositius ja adquirits, de totes maneres, aquesta idea ha estat útil per implantar-se en el sensor de creació propi esmentat del grup bonÀrea.

DESCRIPCIÓ	COMANDA AT
Activació o desactivació del mode alarma.	AT+WMOD=1 1: Enable 0: Disable
Interval de comprovació del rang d'alarma.	AT+CITEMP=1 1: Interval de temps en minuts.

Taula 13: Comandes per a la utilització del futur Alarm Mode.

- Període de transmissió:

Per defecte el període de captació i transmissió del sensor establert és de 10 minuts, degut a la pretensió d'utilitzar el Mode Alarma i per minimitzar el desgast de la bateria aquest es va establir en 20 minuts, d'aquesta forma durant el procés de prova de funcionament del sistema s'obtenien dades en temps no excessivament prolongats

però tampoc excessivament curts, permetent l'edició i realització de canvis en l'arquitectura del sistema entre períodes.

Descripció	Comanda AT
Set Record Time Period	AT+RTP

Pel que respecta a altres especificacions aquestes han estat definides a 4.2 i principalment cal destacar la utilització de Clase A i OTAA. El mètode de connexió a la xarxa, una vegada amb les claus OTAA corresponents registrades a la gateway no ha estat més que prémer el polsador ACT durant aproximadament 5 segons, i trobant-nos en una zona amb cobertura el sensor s'ha connectat automàticament. Un fet a tenir en compte detectat en el període de prova de la instal·lació ha estat que si es connecta el sensor a la xarxa i s'instal·la en un punt amb escassa cobertura, a banda de la possible pèrdua de paquets existeix la possibilitat que aquest es desconnecti i no sigui capaç de connectar-se de nou a la xarxa. Per tant, caldrà ser curosos amb la cobertura quan la instal·lació augmenti en nombre de dispositius.

Finalment a la taula adjunta es detalla els rangs de nivells de senyal RSSI, una dada que correspon al sensor i que es representada a l'eina visual d'aquesta instal·lació.

RSSI	Descripció
-30 dBm	Màxima intensitat de senyal, en aquest cas la gateway i el sensor estaran molt propers.
-67 dBm	Nivell mínim de senyal per a aplicacions que necessitin poc delay, com VoIP o streaming de vídeo.
-70dBm	Mínim de senyal per a entrega de paquets fiable.
-80 dBm	Possible pèrdua de paquets i mínim per a que la connectivitat sigui fiable.
-90dBm	Difícilment funcionarà la comunicació.

Taula 14: Nivell de senyal RSSI i significat.

8. CONCLUSIONS

Amb el projecte finalitzat i fent memòria del transcurs d'aquest, on s'hi ha dedicat aproximadament sis mesos, són força i variades les conclusions que se'n poden extreure, tant en l'àmbit personal com tècnic.

Vaig iniciar aquest projecte sent coneixedor que era un repte molt interessant i amb molt per aprendre, però amb la intenció d'ampliar els coneixements adquirits durant el grau i conèixer com és el desenvolupament d'un projecte dins una empresa de primera mà. El procés d'aquest ha tingut etapes complicades, però també etapes de gran satisfacció, les primeres sobretot durant el transcurs de configuració de la gateway, on els nous conceptes d'un camp basat en gran mesura a la informàtica i telecomunicacions es van haver de digerir sense pressa, però sense pausa. Per altra banda el fet de distingir el projecte en etapes, cada consecució d'aquestes provocava satisfacció i ànims per seguir amb la següent. Així doncs aquest procés m'ha dut a entendre un gran nombre de conceptes i eines que seran útils en pròximes tasques que es realitzin en l'empresa, però també en la comprensió de nous camps com a enginyer.

Per altra banda cal destacar la particularitat de la xarxa que s'ha creat, a diferència del que podem trobar generalment en aquest cas no s'ha fet ús en cap moment del Cloud, sinó que s'ha aconseguit realitzar-ho de forma local, amb l'abaratiment que suposa això en el desplegament i manteniment de la xarxa i la seguretat que hi aporta. Tanmateix no s'ha fet ús de TTN, sinó que s'ha gestionat el servidor i el tractament de les dades, també, de forma local.

A nivell de concepte cal esmentar que durant el transcurs del projecte es van tindre dubtes de si realment aquesta tecnologia era viable per a la finalitat desitjada. Aquests dubtes van sorgir quan un es va adonar que aquesta tecnologia està dirigida al monitoratge de dades, i que aquí és on es fonamenta la durada de la bateria dels sensors sense fil que utilitza. Per tant, la idea de realitzar un control de temperatures en intervals de temps molt curts no tenia sentit. Aquest fet es solucionarà mitjançant l'opció de la qual disposaran sensors que utilitzen aquesta tecnologia, que és forçar l'enviament d'un missatge quan es sobrepassa, en aquest cas, una temperatura concreta.

A nivell de xarxa caldrà donar continuïtat al desenvolupament d'aquesta, tenint en compte que en algunes zones la cobertura és escassa, i que tindrà un límit pel que fa a la quantitat de nodes finals que la gateway actual podrà gestionar. En aquest cas la solució d'un problema implicarà la solució de l'altre, ja que caldrà crear una xarxa de gateway ja sigui amb un servidor central o amb servidors segons la zona o finalitat. Si bé existeix la possibilitat d'instal·lar amplificadors de xarxa LoRaWAN, aquests no seran viables si com es pretén, es sobrepassa una quantitat de dispositius d'aproximadament 5.000.

Així doncs, sense ser-ne conscient en un inici, m'he trobat immers en un camp veritablement interessant alhora que complex, tot i treballar amb dispositius d'un nivell força professional

existeixen moltes altres opcions, de tots els preus i gustos. Per tant el procés d'aprenentatge no acaba aquí.

En definitiva, ha estat un procés complex, potser més del que pugui semblar, per a un estudiant d'enginyeria electrònica que disposava dels coneixements adquirits al grau en aquest àmbit. Tant o més satisfactori que complex n'és el resultat a escala personal, sent conscient que el projecte no finalitza aquí, sinó que el pròxim pas és establir-lo a l'empresa juntament amb altres aplicacions que utilitzin aquesta tecnologia, però això requerirà de gestions i inversions a realitzar, amb els processos que això comporta.

9. TREBALLS FUTURS

Són varis els treballs futurs possibles que es podran aplicar en aquest projecte, tant a nivell de xarxa com de conceptes, aquests són els següents:

- Tractant-se d'una tecnologia relativament moderna i que engloba una gran quantitat de conceptes, serà molt interessant seguir en el procés d'aprenentatge, per tal de en un futur i en mesura del possible implementar noves, millors i eficients solucions.
- A banda de LoRa i LoRaWAN s'entra en el món de la IoT, on no només aquestes dues tecnologies en formen part. Per tant a nivell més global s'obren noves oportunitats.
- Estudiar com s'haurà de dur a terme l'ampliació de la xarxa, així com la gestió de grans quantitats de dades sigui segons la zona de procedència o el seu significat.
- Aquesta primera instal·lació ha estat utilitzada com a prova pilot, però són moltíssimes les aplicacions que es poden realitzar amb aquesta tecnologia. Des del grup bonÀrea ja s'està treballant en algunes d'aquestes, com són:
 - Lectura del nivell de pinso en sitges de les granges.
 - Detecció de fuites d'oli en maquinària pertanyent a cadenes de producció.
 - Lectura del diferencial i tèrmic dels molls de càrrega dels camions refrigerats.
 - Lectura d'un detector termovelocimètric amb sortida digital per connectar-ho al sensor propi bonÀrea.
- En aquest projecte s'utilitza un change node a Node-RED per tal de canviar l'identificador de cada sensor DevEUI per un nom desitjat i que defineixi aquest sensor. És obvi que en una instal·lació amb milers de sensors no resultaria una opció eficient, i per tal de solucionar aquest fet es podria realitzar la lectura d'un fitxer CSV extern on es relacionés el DevEUI amb el nom desitjat, i mitjançant una funció és realitzes el canvi de nom entre aquests.

Aquest però, és un fet el qual no s'ha treballat en aquest projecte ja que el grup empresarial està desenvolupant el seu sensor propi, el qual disposarà del camp NAME en el seu missatge, que es definirà quan es programi el sensor corresponent.
- Estudiar la necessitat de realitzar un mapa de nivells de cobertura, així com la distància mínima a partir del qual el node final rebrà senyal directa de l'antena i no una senyal reflectida.

10. BIBLIOGRAFÍA

- [1]. Google Maps.
<https://www.google.es/maps/>
- [2]. ¿Qué es la red lora?
<https://deepdata.es/red-lora>
- [3]. Figure 3.
https://www.researchgate.net/figure/a-LoRaWAN-network-architecture-and-b-LoRaWAN-protocol-stack_fig3_326134076
- [4]. Fundamentos de node-red.
<https://www.techedgegroup.com/es/blog/fundamentos-node-red>
- [5]. Qué es un sistema SCADA, para qué sirve y cómo funciona.
<https://www.cursosaula21.com/que-es-un-sistema-scada/>
- [6]. Help WinCC OA.
https://www.winccoa.top/help3111/WebHelp/wincc_oa.htm
- [7]. Multitech Conduit IP67 Base Station Manual.
<https://www.multitech.com/documents/publications/data-sheets/86002197.pdf>
- [8]. Conduit Base Station IP 67 Getting Started Guide.
<https://www.multitech.com/documents/publications/manuals/S000665.pdf>
- [9]. LHT65 LoRaWAN Temperature & Humidity Sensor.
<https://www.dragino.com/products/lora-lorawan-end-node/item/151-lht65.html>
- [10]. LHT65 User Manual.
https://www.dragino.com/downloads/downloads/LHT65/UserManual/LHT65_Temperature_Humidity_Sensor_UserManual_v1.3.pdf
- [11]. Protocolo TCP/IP – Qué es y cómo funciona.
<https://www.profesionalreview.com/2020/03/21/protocolo-tcp-ip/>
- [12]. ¿Qué es MQTT? Su importancia como protocolo IoT.
<https://www.luisllamas.es/que-es-mqtt-su-importancia-como-protocolo-iot/>
- [13]. Multitech Support Portal.
<https://support.multitech.com/support/login.html>
- [14]. Node-RED Forum.
<https://discourse.nodered.org/>
- [15]. SIMATIC WinCC Open Architecture Portal.
<https://www.winccoa.com/forum/>
- [16]. Grafana Labs Community Forums.
<https://community.grafana.com/>
- [17]. The Things Network.
<https://www.thethingsnetwork.org/>
- [18]. The Things Network Documentation.
<https://www.thethingsnetwork.org/docs/>
- [19]. Qué es Node-Red y para que sirve.
<https://iotconsulting.tech/que-es-node-red-y-para-que-sirve/>

- [20]. NODE-RED: Construye el Internet de las Cosas.
<https://ricveal.com/blog/node-red-construye-el-internet-de-las-cosas>
- [21]. Tag LoRaWAN a Aprendiendo Arduino.
<https://www.aprendiendoarduino.com/tag/lorawan/>
- [22]. Tag TTN a Aprendiendo Arduino.
<https://www.aprendiendoarduino.com/tag/ttn/>
- [23]. LoRaWAN una red de largo alcance para IoT.
<http://www.iot-partners.com/2015/12/lorawan-una-red-de-largo-alcance-para-iot/>
- [24]. Haciendo IoT con LoRa.
<https://medium.com/beelan/haciendo-iot-con-lora-cap%C3%ADtulo-1-qu%C3%A9-es-lora-y-lorawan-8c08d44208e8>
- [25]. Tecnología LoRa y LoRaWAN.
<https://www.catsensors.com/es/lorawan/tecnologia-lora-y-lorawan>
- [26]. Desarrollar con LORa para aplicaciones IoT de baja tasa y largo alcance.
<https://www.digikey.es/es/articles/develop-lora-for-low-rate-long-range-iot-applications>
- [27]. SCADA: qué es y sus beneficios.
<https://paradiso-fp7.eu/scada/>
- [28]. ¿Qué es SCADA?
<https://www.wonderware.es/hmi-scada/que-es-scada/>
- [29]. Los sistemas SCADA en la automatización industrial.
<file:///C:/Users/ASUS/Downloads/Dialnet-LosSistemasSCADAEnLaAutomatizacionIndustrial-5280242.pdf>
- [30]. SIMATIC WinCC OA.
<https://new.siemens.com/global/en/products/automation/industry-software/automation-software/scada/simatic-wincc-oa.html>
- [31]. Desarrollo de SCADAs. Introducción a WinCC Open Architecture.
<https://www.sothis.tech/desarrollo-de-scadas-introduccion-a-wincc-open-architecture/>
- [32]. OPC UA.
<https://www.logicbus.com.mx/blog/opc-ua/>
- [33]. ¿Que es OPC UA?
<https://www.opiron.com/que-es-opc-ua/>
- [34]. Protocolo TCP/IP – Qué es y cómo funciona.
<https://www.profesionalreview.com/2020/03/21/protocolo-tcp-ip/>
- [35]. Qué es TCP/IP.
<https://openwebinars.net/blog/que-es-tcpip/>
- [36]. Los Protocolos TCP/IP.
http://www.juntadeandalucia.es/empleo/recursos/material_didactico/especialidades/materialdidactico_administrador_servidores/Content/2-redes_tcp/3-LosProtocolosTCP-IP.pdf

- [37]. MQTT, Qué es, ¿cómo se puede usar? Y cómo funciona.
<https://descubrearduino.com/mqtt-que-es-como-se-puede-usar-y-como-funciona/>
- [38]. ¿Qué es MQTT?
<https://www.indelmar.com/?p=1140>
- [39]. Multitech Conduit IP67 Base Station.
<https://www.multitech.com/brands/multiconnect-conduit-ip67>
- [40]. Multitech Conduit IP67 Base Station.
<https://shop.connectedyou.io/products/multiconnect%C2%AE-conduit-ip67-base-station>
- [41]. LORAWAN, PRIVATE NETWORK VS PUBLIC NETWORK.
<https://elainnovation.com/lorawan-private-network-vs-public-network-which-one-should-i-choose.html>
- [42]. Grafana, un software de código abierto para análisis y supervisión.
<https://ubunlog.com/grafana-software-analisis-supervision/>
- [43]. Monitorización gratuita con InfluxDB, Telegraf y Grafana.
<https://aleson-itc.com/monitorizacion-gratuita-con-indluxdb-telegraf-y-grafana/>
- [44]. InfluxDB: explicación, ventajas y primeros pasos.
<https://www.ionos.es/digitalguide/hosting/cuestiones-tecnicas/que-es-influxdb/>

11. ANNEX

A) ALTRES CONFIGURACIONS DE LA GATEWAY.

A continuació es descriuen apartats que no s'han modificat durant el transcurs de configuració de la gateway i que per tant s'han deixat per defecte. Aquest fet és degut a que o bé no eren necessaris o s'endinsaven en excés a coneixements molt concrets de la informàtica o telecomunicacions. Aquests fets no impliquen que la continuïtat del projecte no es tinguin en compte.

- Firewall

Firewall és el que coneixem com a Tallafores en català, aquest és un sistema que té com a funció protegir la nostra xarxa d'intrusions o atacs, permetent el tràfic entrant i sortint entre dispositius de una mateixa xarxa. En el cas de la gateway existeix també aquest sistema i és en aquest apartat on l'usuari pot adaptar el tallafores a les seves necessitats, personalitzant tant el filtre d'entrada com el de sortida, ja que la barrera de protecció per defecte és la més bàsica permetent tota sortida de paquets i evitant la entrada d'aquests provinents de xarxes externes.

- SMS:

Aquesta funció permet la interacció amb la gateway mitjançant missatges SMS, aplicant la comanda corresponent podrem fer un reset, ping o rebre configuracions entre altres de la gateway. Per poder utilitzar aquesta opció es necessària la inserció d'una targeta telefònica amb capacitat per rebre i enviar missatges SMS a la zona corresponent de la gateway.

- Tunnels:

Aquesta funció permet gestionar túnels amb protocol GRE, IPsec o OpenVPN. No s'entrarà en detall d'aquests, però s'utilitzen per enviar dades d'una xarxa privada a través d'una xarxa pública.

- Status & Logs:

Tal com el seu nom indica aquest apartat ens serà útil per comprovar els estats i processos de la nostra gateway. Concretament les estadístiques d'aquesta en quant a memòria, nodes finals i paquets de dades entre altres i els estats de serveis com DDNS, SMS, Mail o altres notifikacions.


- Commands:

Aquí podrem guardar, revertir o reinicialitzar els canvis fets en la configuració de la nostra gateway. A més a més podrem reiniciar el dispositiu o només els serveis LoRa.

- Apps:

Permet la gestió de l'app Node-RED desactivada per defecte, també la gestió d'aplicacions personalitzades que caldrà importar des de deviceHQ, on se'n poden observar algunes ja creades.

B) IMATGES DE CONFIGURACIONS EN 7.2.1.



mPower™ Edge Intelligence Conduit - Application Enablement Platform
 MTCDTIP-L4E1-266A Firmware 5.2.1

Home
 Save and Apply
 LoRaWAN ®
 Setup
 Cellular
 Firewall
 SMS
 Tunnels
 Administration
 Status & Logs
 Commands
 Apps
 Help

DEVICE INFORMATION

Device	
Model Number	MTCDTIP-L4E1-266A
Serial Number	20760140
IMEI	351626100036158
Firmware	5.2.1
Current Time	01/19/2021 18:05:51
Up Time	00:07:27
WAN Transport	None
Current DNS	192.168.141.16, 192.168.101.109
GeoPosition	41° 47.3745' 1° 17.0251'

LAN	
Ethernet	(eth0)
Mode	Static
Bridge	—
MAC Address	00:08:00:4A:DF:E0
IPv4 Address	192.168.171.94
Mask	255.255.255.0
DHCP State	Disabled

WAN	
Cellular	(ppp0)
State	Disabled
Signal	

Accessory Cards	
Card1	(AP1)
Model Number	MTAC-LORA-H-868
Serial Number	20730181
Hardware	MTAC-LORA-1.5

LoRaWAN

- Network Settings
- Key Management
- Gateways
- Devices
- Device Groups
- Profiles
- Packets
- Downlink Queue
- Operations
- Setup
- Cellular
- Firewall
- SMS
- Tunnels
- Administration
- Status & Logs
- Commands
- Apps
- Help

LoRa Mode

Mode	Packet Forwarder	Network Server	LoRa Server
NETWORK SERVER	4.0.1-931.0	2.3.12	2.3.12
Status	Status	Status	Status
RUNNING	RUNNING	RUNNING	DISABLED

LoRa Card Information

Gateway EUI	00-80-00-00-A0-00-5C-BD
Frequency Band	868
PPGA Version	31

LoRaWAN Network Server Configuration

Channel Plan

Channel Plan	Additional Channels 1 (MHz)	Duty Cycle Period (min)
EU868	867.5	60
Channel Mask	Edit	

Network

Network Mode	Join Delay (sec)	Lease Time	Address Range Start
Public LoRaWAN	5	00-00-00	00:00:00:01
NetID	Rx1 Delay (sec)	Queue Size	Address Range End
000000	1	16	FFFFFFFFFE

Settings

Tx Power (dBm)	Rx 1 DR Offset	ADR Step (dB)	Min Datarate
26	0	30	0 - SF12BW125
Antenna Gain (dBi)	Rx 2 Datarate	ACK Timeout	Max Datarate
3	0 - SF12BW125	5000	3 - SF9BW125

Class B Settings

☐ Enable Beaconing

☐ Disable Beacon Hopping

☐ Disable Ping Slot Hopping

Beacon Power (dBm)	Beacon Frequency (MHz)	Ping Slot Frequency	Ping Slot Datarate
27	0	0	DEFAULT
Info Descriptor	Beacon Latitude (°)	Beacon Longitude (°)	
0	0	0	

Database

Database Path	Trim Rows	<input type="checkbox"/> Reduce Uplink Writes
/var/config/lora/lora-network-c	100	
Backup Interval	Trim Interval	<input type="checkbox"/> Skip Field Check
3600	600	

Network Server Logging

Output to file should be used for debugging only. Reset to SYSLOG for deployments.

Log Destination	Log Level
SYSLOG	INFO
Path	
/var/log/lora-network-server.log	

Network Server Testing

☐ Disable Join Rx1
☐ Disable Join Rx2
☐ Disable Duty Cycle
☐ Disable GPQ

☐ Disable Rx1
☐ Disable Rx2
☐ Disable Strict Counter

Server Ports

<input type="checkbox"/> Local Only	Network Lead Time
	500
Upstream Port	App Port Up
1780	1784
Downstream Port	App Port Down
1782	1786


Payload Broker

<input checked="" type="checkbox"/> Enabled	Hostname	Username
	127.0.0.1	
	Port	Password
	1883	

[Submit](#)
[Reset To Default](#)

Home

Save and Apply

LoRaWAN 

Network Settings

Key Management

Gateways

Devices

Device Groups

Profiles

Packets

Downlink Queue

Operations

Setup

Cellular

Firewall

SMS

Tunnels


Administration

Status & Logs

Commands

Apps

Help





























































KEY MANAGEMENT 

Join Server

Location

Local Keys

Local End-Device Credentials Add New

Device EUI	App EUI	App Key	Class	Device Profile	Network Profile	Options
11-82-2E-36	41-82-2E-36	****58C852C8	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
91-82-2E-35	51-82-2E-35	****26514867	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
B1-82-2E-1A	A1-82-2E-1A	****4865F816	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
B1-82-2E-0B	B1-82-2E-0B	****F23D4E61	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
00-02-1E-63	41-52-46-32	****5050242F	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
D1-82-2E-72	D1-82-2E-72	****3E683371	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
D1-82-2E-71	81-82-2E-71	****655567BA	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
C1-82-2E-75	91-82-2E-75	****53B99A7E	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
41-82-2E-3D	C1-82-2E-3D	****F6C6117D	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
A1-82-2E-7E	81-82-2E-7E	****74F5CF5E	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
E1-82-2E-73	E1-82-2E-73	****ECF19F37	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
21-82-2E-79	E1-82-2E-79	****C1ED9D1F	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
F1-82-2E-7F	A1-82-2E-7F	****91192AE4	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
C1-82-2E-78	71-82-2E-78	****F8C956CA	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
C1-82-2E-17	71-82-2E-17	****A49D8FE3	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
51-82-2E-07	B1-82-2E-07	****D9428AE4	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
E1-82-2E-08	71-82-2E-08	****9B9297BE	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
C1-82-2E-19	71-82-2E-19	****285D8428	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
51-82-2E-37	31-82-2E-37	****A5194D1E	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
41-82-2E-74	31-82-2E-74	****4D145DBC	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
D1-82-2E-80	A1-82-2E-80	****55A9223B	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
F1-82-2E-09	71-82-2E-09	****1DE88EA6	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
C1-82-2E-81	91-82-2E-81	****B364E5D2	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
F1-82-2E-7D	81-82-2E-7D	****8D5E16D1	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
11-82-2E-0A	81-82-2E-0A	****6357F18F	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
91-82-2E-70	D1-82-2E-70	****A9464E5C	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
F1-82-2E-77	61-82-2E-77	****DAB817FB	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
51-82-2E-76	D1-82-2E-76	****CA5A253F	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
B1-82-2E-18	E1-82-2E-18	****4942A1A3	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 
F1-82-2E-34	B1-82-2E-34	****AECF5E24	A	LW102-OTA-EU868	DEFAULT-CLASS-A	 

Local Network Settings

☒ Enabled

Network ID (AppEUI)

Name

MTCDT-20760140

Default Profile

DEFAULT-CLASS-A

Network Key (AppKey)

Passphrase

MTCDT-20760140

Submit

Reset To Default

Home
Save and Apply
LoRaWAN ®
Network Settings
Key Management
Gateways
Devices
Device Groups
Profiles
Packets
Downlink Queue
Operations
Setup
Cellular
Firewall
SMS
Tunnels
Administration
Status & Logs
Commands
Apps
Help

GATEWAYS 2 Refresh

Gateway EUI	IP Address	IP Port	Version	Last Seen	Options
00-80-00-00-a0-00-5c-bd	127.0.0.1	59618	2	7 seconds ago	

Packets Received 7

Gateways (v1.0 or v1.5)

Gateway EUI	Ch1	Ch2	Ch3	Ch4	Ch5	Ch6	Ch7	Ch8	Ch9	Ch10	CRC	Total
00-80-00-00-a0-00-5c-bd	1	2	3	1	1	2	1	1	0	0	4	12

Duty Cycle Time-On-Air Available (seconds) 7

Gateway EUI	Band 0	Band 1	Band 2	Band 3
00-80-00-00-a0-00-5c-bd	865-868	868-868.6	869.4-869.65	869.7-870
	4.267	4.267	44.865	4.267

Network Statistics 7 Reset

Join Requests Response (ms)

AVG	90%	70%	30%
0	0	0	0

Join Packets

OK	Duplicates	MIC Fails	Unknown	Late	Total
201	5	14368	8	0	14582

Transmitted Packets

Pkt 1st Wnd	Pkt 2nd Wnd	Pkt Ping Slot	ACK Pkts	Total
1596	3	0	50	1599

Join 1st Wnd	Join 2nd Wnd	Join Dropped	Total
199	2	0	201

Received Packets

MIC Fails	Duplicates	CRC Errors	Total
0	0	34547	2241

Scheduled Packets

1st Wnd	2nd Wnd	Ping Slot	Dropped	Total
2235	4	0	0	2239

Home
Save and Apply
LoRaWAN ®
Network Settings
Key Management
Gateways
Devices
Device Groups
Profiles
Packets
Downlink Queue
Operations
Setup
Cellular
Firewall
SMS
Tunnels
Administration
Status & Logs
Commands
Apps
Help

DEVICES 7 Refresh

End Devices Add New

Device EUI	Class	Name	Last Seen	Created	Options
a8-40-41-ae-91-82-2e-35	A		unknown	3 months ago	
a8-40-41-32-11-82-2e-36	A		unknown	3 months ago	
a8-40-41-76-41-82-2e-74	A		unknown	3 months ago	
00-18-b2-00-00-02-1e-63	A		unknown	3 months ago	
a8-40-41-86-c1-82-2e-17	A		unknown	3 months ago	
a8-40-41-52-c1-82-2e-75	A		unknown	3 months ago	
a8-40-41-44-e1-82-2e-08	A		2 minutes ago	3 weeks ago	
a8-40-41-5c-51-82-2e-07	A		1 hour ago	3 weeks ago	
a8-40-41-97-d1-82-2e-71	A		4 minutes ago	5 days ago	
a8-40-41-6b-f1-82-2e-77	A		unknown	5 days ago	

10 records

Sessions Add New

Device EUI	Dev Addr	Up FCnt	Down FCnt	Last Seen	Joined	Details
a8-40-41-ae-91-82-2e-35	00c46c5d	4	0	unknown	local	
a8-40-41-32-11-82-2e-36	0141764d	3	0	unknown	local	
a8-40-41-76-41-82-2e-74	001ee36d	4	0	unknown	local	
00-18-b2-00-00-02-1e-63	01f4a82b	7	8	unknown	local	
a8-40-41-86-c1-82-2e-17	00920d0c	0	0	unknown	local	
a8-40-41-52-c1-82-2e-75	019ef3aa	8	6	unknown	local	
a8-40-41-44-e1-82-2e-08	00444f61	8	0	2 minutes ago	local	
a8-40-41-5c-51-82-2e-07	0035dd11	320	44	1 hour ago	local	
a8-40-41-97-d1-82-2e-71	01bb34fc	386	39	4 minutes ago	local	
a8-40-41-6b-f1-82-2e-77	01a8bd82	0	0	unknown	local	

10 records

Home

Save and Apply

LoRaWAN ®

Network Settings

Key Management

Gateways

Devices

Device Groups

Profiles

Packets

Downlink Queue

Operations

Setup

Cellular

Firewall

SMS

Tunnels

Administration

PROFILES

Refresh

End-Device Profiles ⑦

Add New

Profile ID	Max EIRP	Max Duty Cycle	MAC Version	Supports B	Timeout B	Supports C	Timeout C	Options
LW102-OTA-US915	DEFAULT	DEFAULT	1.0.2	false	DEFAULT	true	DEFAULT	
LW102-OTA-AU915	DEFAULT	DEFAULT	1.0.2	false	DEFAULT	true	DEFAULT	
LW102-OTA-EU868	DEFAULT	DEFAULT	1.0.2	false	DEFAULT	true	DEFAULT	
LW102-OTA-AS923	DEFAULT	DEFAULT	1.0.2	false	DEFAULT	true	DEFAULT	
LW102-OTA-IN865	DEFAULT	DEFAULT	1.0.2	false	DEFAULT	true	DEFAULT	
LW102-OTA-KR920	DEFAULT	DEFAULT	1.0.2	false	DEFAULT	true	DEFAULT	

Network Profiles ⑦

Add New

Profile ID	Rx1 Delay	Rx1 DR Offset	Rx2 DR	Rx2 Frequency	Max Duty Cycle	Class	Timeout C	Options
DEFAULT-CLASS-A	DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT	A	DEFAULT	
DEFAULT-CLASS-B	DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT	B	DEFAULT	
DEFAULT-CLASS-C	DEFAULT	DEFAULT	DEFAULT	DEFAULT	DEFAULT	C	DEFAULT	

Save and Apply

LoRaWAN ®

Network Settings

Key Management

Gateways

Devices

Device Groups

Profiles

Packets

Downlink Queue

Operations

Setup

Cellular

Firewall

SMS

Tunnels

Administration

Status & Logs

Commands

Apps

Help

PACKETS ⑦

Packets ⑦

Records: 10 Page: 1

Device EUI	Freq	Datarate	SNR	RSSI	Size	FCnt	Type	Tx/Rx Time	Details
a8-40-41-44-e1-82-2e-08	867.500	SF12BW125	-1	-111	24	00000008	UpUnc	18:06:22	
a8-40-41-97-d1-82-2e-71	867.300	SF9BW125	13	-79	24	00000182	UpUnc	18:04:03	
a8-40-41-5c-51-82-2e-07	868.500	SF10BW125	-12	-116	24	00000140	UpUnc	17:06:38	
a8-40-41-44-e1-82-2e-08	867.700	SF12BW125	-9	-115	24	00000005	UpUnc	17:06:22	
a8-40-41-97-d1-82-2e-71	868.300	SF9BW125	12	-79	24	0000017F	UpUnc	17:04:03	
a8-40-41-44-e1-82-2e-08	868.500	SF12BW125	-15	-115	24	00000004	UpUnc	16:52:45	
a8-40-41-44-e1-82-2e-08	867.300	SF12BW125	-16	-114	24	00000002	UpUnc	16:52:16	
a8-40-41-44-e1-82-2e-08	867.100	SF12BW125	-15	-115	24	00000001	UpUnc	16:51:45	
a8-40-41-44-e1-82-2e-08	867.500	SF12BW125	4	-104	24	00000000	UpUnc	16:50:48	
a8-40-41-44-e1-82-2e-08	868.500	SF7BW125	-	-	33	00000000	JnAcc	16:50:46	

Showing 1 to 10 of 202 records

Recent Join Requests ⑦

JoinEUI	DevEUI	Nonce	Elapsed (ms)	Result
a8-bb-cc-dd-ee-ff-11-22	00-04-a3-0b-00-1f-ab-8a	30001	0	UnknownDevEUI
a8-bb-cc-dd-ee-ff-11-22	00-04-a3-0b-00-1f-ab-8a	10220	0	UnknownDevEUI
a8-bb-cc-dd-ee-ff-11-22	00-04-a3-0b-00-1f-ab-8a	21036	0	UnknownDevEUI
a8-bb-cc-dd-ee-ff-11-22	00-04-a3-0b-00-1f-ab-8a	19546	0	UnknownDevEUI
a8-bb-cc-dd-ee-ff-11-22	00-04-a3-0b-00-1f-ab-8a	28364	0	UnknownDevEUI
a8-bb-cc-dd-ee-ff-11-22	00-04-a3-0b-00-1f-ab-8a	9716	0	UnknownDevEUI

6 records

Recent Rx Packets ⑦

Records: 10 Page: 1

Tmst	Freq	Datarate	CRC	SNR	RSSI	Size	Type	Data	Details
69207764	868.300	SF12BW125	OK	-20	-115	23	JnReq	ACIR/+7dzLuqiqsfAAujBA	
153906172	868.100	SF12BW125	OK	-1.5	-117	23	JnReq	ACIR/+7dzLuqiqsfAAujBA	
173656916	867.500	SF7BW125	ERR	-12	-114	87	Unknown	6pyKiGSDP8Nviej5Wv9sy'	
223970732	867.900	SF7BW125	ERR	-11.8	-115	153	Unknown	ko44vcHyYESP9Y8dUDDr	
227321604	867.300	SF9BW125	OK	13.8	-79	24	UpUnc	QPw0uwGAggECikn+IZDg	
238609492	868.500	SF12BW125	OK	-6.5	-115	23	JnReq	ACIR/+7dzLuqiqsfAAujBA	
261360955	867.100	SF7BW125	OK	-4.2	-115	40	UpUnc	QPBhASaAx4CoDJr/JqL	
323300164	868.500	SF12BW125	OK	-1.8	-116	23	JnReq	ACIR/+7dzLuqiqsfAAujBA	
366105612	867.500	SF11BW125	OK	-1.8	-111	24	UpUnc	QGFPRACACACz6p840V	
380827667	868.500	SF7BW125	ERR	-11.5	-116	92	Unknown	CJoVTZXBcRE+dGla45f/V	

Showing 1 to 10 of 13 records

Home
Save and Apply
LoRaWAN
Network Settings
Key Management
Gateways
Devices
Device Groups
Profiles
Packets
Downlink Queue
Operations
Setup
Cellular
Firewall
SMS
Tunnels
Administration
Status & Logs
Commands
Apps
Help

OPERATIONS
Schedule Progress

Operation Settings

Operation Type

FOTA

Firmware Upgrade File...

No file selected

Fragment Description (HEX)

00000000

Transmission Setup & Launch Date/Time Selection

Show Settings

Current Date/Time

Tue Jan 19 2021 18:09:34 GMT+0100 (hora estándar de Europa central)

Setup Date/Time

Tue Jan 19 2021 18:09:34 GMT+0100 (hora estándar de Europa central)

Launch Date/Time

Tue Jan 19 2021 18:10:34 GMT+0100 (hora estándar de Europa central)

Setup Time In

0 seconds

Launch Time In

60 seconds

Setup Time Input

Countdown To Setup From Setup

Number of Days

0

HH:MM:SS

0

Launch Time Input

Countdown To Launch From Setup

Number of Days

0

HH:MM:SS

60

(from setup time)

(from setup time)

Target End-Devices

End-device Group

Group Name	EUI	Size
No matching records		

Submit

Home
Save and Apply
LoRaWAN
Setup
Network Interfaces
WAN Configuration

NETWORK INTERFACES CONFIGURATION
Reset To Default

Name	Direction	Type	IP Mode	IP Address	Bridge	Options
eth0	LAN IPv4	ETHER	Static	192.168.171.94/24	--	
ppp0	WAN IPv4	PPP	PPP			
br0	LAN IPv4	BRIDGE	Static	192.168.2.1/24	br0	

Home
Save and Apply
LoRaWAN
Setup
Cellular
Firewall
SMS
Tunnels
Administration
User Accounts
Self-Diagnostics (beta)
Access Configuration
RADIUS Configuration
X.509 Certificate

LOCAL USER ACCOUNTS
Add New User Change Your Password Change Password Complexity Rules

Enabled	Username	Role	Creation Date	Last Login	Password Changed	Options
<input checked="" type="checkbox"/>	admin	administrator	12/25/2020 09:12:36	01/19/2021 18:05:19	never	

One record

Home
Save and Apply
LoRaWAN ®
Setup
Cellular
Firewall
SMS
Tunnels
Administration
User Accounts
Self-Diagnostics (beta)
Access Configuration
RADIUS Configuration
X.509 Certificate
X.509 CA Certificates
Remote Management
Notifications
Web UI Customization
Firmware Upgrade
Save/Restore
Debug Options
Usage Policy
Support
Status & Logs
Commands
Apps
Help

ACCESS CONFIGURATION ⓘ

Web Server

HTTP Redirect to HTTPS

☒ Enabled
☒ Via LAN
☒ Via WAN

Port

80

HTTPS

☒ Via WAN

Port

443

Authorization

Session Timeout (minutes)

20

HTTPS Security

Show i

SSH Settings

☒ Enabled

Port

22

☒ Via LAN
☐ Via WAN

SSH Security

Show i

Reverse SSH Tunnel

☐ Enabled

Server

Remote Port

2222

Username

Authentication Method

Password

Password

.....

👁

ICMP Settings

☒ Enabled
☒ Respond to LAN
☐ Respond to WAN

Node-RED Settings

☒ Via LAN
☒ Via WAN

SNMP Settings

☒ Via LAN
☐ Via WAN

Modbus Slave

☐ Enabled
☐ Via LAN

Port

1502

IP Defense

DoS Prevention

☒ Enabled

Per Minute

60

Burst

100

Ping Limit

☒ Enabled

Per Second

10

Burst

30

Brute Force Prevention

☒ Enabled

Attempts

3

Lockout Minutes

5

Bootloader Protection

Show i

Submit

Reset To Default

90

MULTITECH mPower™ Edge Intelligence Conduit - Application Enablement Platform
 MTCOTIP-L4E1-266A Firmware 5.2.1

Home
 Save and Apply
 LoRaWAN ®
 Setup
 Cellular
 Firewall
 SMS
 Tunnels
Administration
 User Accounts
 Self-Diagnostics (beta)
 Access Configuration
 RADIUS Configuration
 X.509 Certificate
 X.509 CA Certificates
Remote Management
 Notifications
 Web UI Customization
 Firmware Upgrade
 Save/Restore
 Debug Options
 Usage Policy
 Support
 Status & Logs
 Commands
 Apps

REMOTE MANAGEMENT ⓘ

Remote Server

☐ Enabled
☒ SSL Enabled
 Account Key

DeviceHQ Check-In Settings ⓘ

☒ Intervals Check-In Interval (minutes) GPS Data Interval (minutes)
☐ Single Check-In Date Time
☐ Repeatable Repeat Time

Update Settings

☐ Sync with Dial-On-Demand ☒ Allow Firmware Upgrade
☒ Allow Configuration Upgrade ☐ Allow Configuration Upload

DeviceHQ App Server

App Store URL

Status

Current Time	19/1/2021 18:11:28	Current Status	unknown
Last Check-In	unknown	Tip: Trigger checkin via SMS by configuring SMS Commands .	
Next Check-In	unknown		

Submit **Reset To Default**

MULTITECH mPower™ Edge Intelligence Conduit - Application Enablement Platform
 MTCOTIP-L4E1-266A Firmware 5.2.1

Home
 Save and Apply
 LoRaWAN ®
 Setup
 Cellular
 Firewall
 SMS
 Tunnels
Administration
 User Accounts
 Self-Diagnostics (beta)
 Access Configuration
 RADIUS Configuration
 X.509 Certificate
 X.509 CA Certificates
 Remote Management
 Notifications
 Web UI Customization
 Firmware Upgrade
Save/Restore
 Debug Options

SAVE AND RESTORE CONFIGURATION ⓘ

Save and Restore Configuration

Restore Configuration From File **Restore** **Browse...** No file selected
 Save Configuration To File **Save**
 Reset to User-Defined Configuration **Reset**

User-Defined Default

Set Current Configuration As User-Defined Default **Set**
 Clear User-Defined Default **Clear**

User-defined default configurations are used to set deployment-specific default settings, overriding the factory default configurations. When the RESET button on the device is held for 5 seconds, the unit will be reset to the user-defined default settings if set, otherwise factory default settings.

To override user-defined default configurations and restore the unit to factory default, press and hold the RESET button on the device for 30 seconds.

Home
Save and Apply
LoRaWAN ®
Setup
Cellular
Firewall
SMS
Tunnels
Administration
Status & Logs
Statistics
Services
Mail Log
Home
Save and Apply
LoRaWAN ®
Setup
Cellular
Firewall
SMS
Tunnels
Administration
Status & Logs
Statistics
Services
Mail Log
Mail Queue
Notifications Sent

STATISTICS ?
System Ethernet Cellular GRE IPsec OpenVPN LoRa

Model Number MTCDTIP-L4E1-266A
Firmware Information 5.2.1 2020-05-26T09:19:10
System Uptime 00:14:22
Mac-Address 00:08:00:4A:DF:E0

Memory Usage

	Total	Used	Free	Available	Shared	Buff/Cache
Memory	246.64 MB	86.59 MB	107.95 MB	151 MB	1.48 MB	52.1 MB
Swap	0 Bytes	0 Bytes	0 Bytes			
Total	246.64 MB	86.59 MB	107.95 MB			

System Log
[show 1](#)
[Download Logs](#)
Last updated: 18:12:45

SERVICE STATISTICS ?

Service Name	Configuration	Status
DDNS	Disabled	DDNS is disabled
SNTP	Enabled	Failed to synchronize: 19 Jan 18:12:57 ntpdate[7276]: no server suitable for synchronization found
TCP/ICMP Keep Alive	Disabled	PING Keep alive is disabled
Dial-On-Demand	Disabled	PPP is not running
SMTP	Disabled	SMTP is disabled
SMS	Disabled	SMS is disabled
Failover	Enabled	Failover service is running

Last Updated: 18:13:06

MULTITECH
mPower™ Edge Intelligence Conduit - Application Enablement Platform
MTCDTIP-L4E1-266A Firmware 5.2.1

Home
Save and Apply
LoRaWAN ®
Setup
Cellular
Firewall
SMS
Tunnels
Administration
Status & Logs
Commands
Apps
Help

MANAGE APPS ?
[Launch Node-RED](#)

Node-RED Apps
☒ Enabled

Name	Version	Status	Actions
Development	0.0.0	Running	🔗

Custom Apps
[Add Custom App](#)
☒ Enabled ☒ Backup On Install

Name	Version	Status	Info	Actions
No items found.				

C) IMATGES DE LA INSTAL·LACIÓ





D) ADEUNIS LORAWAN FTD.

Un element molt important quan es creen xarxes de comunicació és analitzar-ne la seva cobertura en els indrets desitjats, durant la realització d'aquest projecte s'han estudiat opcions per a realitzar un mapa de cobertures de la instal·lació, les quals no s'han dut a terme ja que necessitaven d'una inversió considerable no prevista, alhora que en el cas que ens ocupa no resultaven d'elevada importància, ja que la intenció era observar la funcionalitat de la xarxa per posteriorment, si aquesta aportava els resultats esperats augmentar-ne la capacitat i a conseqüència la cobertura. Tot i aquest fet un dels dispositius assequibles per a realitzar proves de cobertures ha estat el dispositiu de la marca Adeunis per a proves de cobertura en camp en xarxes LoRaWAN el qual permet transmetre, rebre i visualitzar instantàniament el nivell de senyal en dbm en un punt en concret de la nostra xarxa.

Tant el seu disseny com el seu funcionament són força senzills, ja que ens trobem amb una pantalla LCD, un pulsador per enviar el missatge i un altre pulsador al lateral per canviar entre pantalles. Pel que fa a les diferents pantalles a la primera podrem observar el nivell de senyal ascendent i descendent en format gràfic, a diferència de la segona que ens indicarà el mateix però amb nivell db. Per altra banda incorpora una tercera pantalla relacionada amb l'anàlisi mitjançant GPS, la seva funció és crear un mapa automàticament amb les zones testejades on ha arribat la cobertura però aquesta no es va utilitzar ja que aquest tipus de senyal no es percep dins la majoria de naus del complex industrial. La quarta i última pantalla ens indica els errors de transmissió de paquets, és a dir, la quantitat de paquets rebuts respecte als enviats en format numèric i tant per cent.

